



ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ

ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΤΕΥΧΟΣ ΔΕΥΤΕΡΟ Αρ. Φύλλου 88

26 Ιανουαρίου 2005

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΠΟΦΑΣΕΙΣ

ΑΠΟΦΑΣΕΙΣ

Αριθ. 632 α (1)

Κανονισμός για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές.

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΑΔΕΑ)

Έχοντας υπόψη :

α. Το Ν. 3115/27.2.2003, άρθρο 1, παραγρ. 1.

β. Το Ν. 3115/27.2.2003, άρθρο 6, παραγρ. 1.

γ. Ότι εκ της αποφάσεως δεν προκύπτει δαπάνη για το δημόσιο.

δ. Τη σχετική εισήγηση της Υπηρεσίας, αποφάσισε:

Κατά τη συνεδρίασή της την 10η Νοεμβρίου 2004, την έγκριση του παρακάτω Κανονισμού για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές.

ΚΕΦΑΛΑΙΟ Ι
ΣΚΟΠΟΣ - ΟΡΙΣΜΟΙ

Άρθρο 1
Σκοπός - Πεδίο Εφαρμογής

1. Σκοπός του παρόντος Κανονισμού είναι:

(α) Η διασφάλιση του απορρήτου των διαδικτυακών επικοινωνιών.

(β) Η ασφάλεια των διαδικτυακών τηλεπικοινωνιακών φορέων και Δημοσίων οργανισμών.

(γ) Η θέσπιση των υποχρεώσεων των εν λόγω φορέων αναφορικά με την ασφάλεια και το απόρρητο των επικοινωνιών.

(δ) Ο έλεγχος στους εν λόγω φορείς σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

2. Στις διατάξεις του παρόντος Κανονισμού εμπίπτουν όλοι οι Τηλεπικοινωνιακοί Φορείς Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα:

(α) Πάροχοι πρόσβασης στο Διαδίκτυο (σταθεροί και κινητοί τηλεπικοινωνιακοί πάροχοι, Internet Service Providers κλπ.)

(β) Πάροχοι διαδικτυακών υπηρεσιών

(γ) Πάροχοι διαδικτυακών υπηρεσιών προστιθέμενης αξίας.

Άρθρο 2
Ορισμοί

Για την εφαρμογή του παρόντος Κανονισμού οι ακόλουθοι όροι έχουν την έννοια που τους αποδίδεται κατωτέρω:

Δίκτυο ηλεκτρονικών επικοινωνιών: τα συστήματα μετάδοσης και, κατά περίπτωση, ο εξοπλισμός μεταγωγής ή δρομολόγησης και οι λοιποί πόροι που επιτρέπουν τη μεταφορά σημάτων, με τη χρήση καλωδίου, ραδιοσημάτων, οπτικού ή άλλου ηλεκτρομαγνητικού μέσου, συμπεριλαμβανομένων των δορυφορικών δικτύων, των σταθερών (μεταγωγής δεδομένων μέσω κυκλωμάτων και πακετομεταγωγής, συμπεριλαμβανομένου του Διαδικτύου) και κινητών επίγειων δικτύων, των συστημάτων ηλεκτρικών καλωδίων, εφόσον χρησιμοποιούνται για τη μετάδοση σημάτων, των δικτύων που χρησιμοποιούνται για ραδιοτηλεοπτικές εκπομπές, καθώς και των δικτύων καλωδιακής τηλεόρασης, ανεξάρτητα από το είδος των μεταφερόμενων πληροφοριών.

Υπηρεσίες ηλεκτρονικών επικοινωνιών: οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις. Στις υπηρεσίες ηλεκτρονικών επικοινωνιών δεν περιλαμβάνονται υπηρεσίες παροχής ή ελέγχου περιεχόμενου που μεταδίδεται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και

υπηρεσίες της κοινωνίας της πληροφορίας, όπως αυτές ορίζονται στην παράγραφο 2 του άρθρου 2 του Π.Δ. 39/2001 (Α΄ 28), και που δεν αφορούν, εν όλω ή εν μέρει, τη μεταφορά σημάτων σε δίκτυα επικοινωνιών.

Διαδικτυακές επικοινωνίες: Υπηρεσίες ηλεκτρονικών επικοινωνιών όπου το δίκτυο ηλεκτρονικών επικοινωνιών είναι δίκτυο μετάδοσης δεδομένων και φωνής με πακετομεταγωγή το οποίο είτε έχει τη μορφή ενδοδικτύου (Intranet) είτε είναι ολόκληρο το Διαδίκτυο (Internet).

Παροχή δικτύου διαδικτυακών επικοινωνιών: η σύσταση, η λειτουργία, ο έλεγχος και η διάθεση τέτοιου δικτύου.

Πάροχος δικτύου διαδικτυακών επικοινωνιών: Η επιχείρηση ή το νομικό πρόσωπο που παρέχει δίκτυο διαδικτυακών επικοινωνιών ή/και το νομικό πρόσωπο που παρέχει στο προσωπικό του την απαραίτητη δικτυακή υποδομή για χρήση διαδικτυακών επικοινωνιών στα πλαίσια της εργασίας του. Για τις ανάγκες του παρόντος ο πάροχος δικτύου διαδικτυακών επικοινωνιών θα αναφέρεται στη συνέχεια του κειμένου ως «πάροχος».

Χρήστης: κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας.

Χρήστης Παρόχου: κάθε φυσικό πρόσωπο που εργάζεται στην επιχείρηση ή στο νομικό πρόσωπο που παρέχει στο προσωπικό του την απαραίτητη δικτυακή υποδομή για χρήση διαδικτυακών επικοινωνιών στα πλαίσια της εργασίας του.

Δεδομένα κίνησης: τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της.

Δεδομένα θέσης: τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.

Συγκατάθεση του χρήστη ή του συνδρομητή: η συγκατάθεση του προσώπου που αφορούν τα δεδομένα, κατά την έννοια της οδηγίας 95/46/ΕΚ.

Υπηρεσία προστιθέμενης αξίας: υπηρεσία μη τηλεπικοινωνιακή η οποία μπορεί να παρέχεται ή να υποστηρίζεται από δίκτυο διαδικτυακών επικοινωνιών.

Πολιτική ασφάλειας: Το σύνολο τεχνικών, οργανωτικών και κανονιστικών μέτρων, τα οποία εφαρμόζονται από πάροχο διαδικτυακών επικοινωνιών και αποβλέπουν στη διασφάλιση του απορρήτου και γενικά στην ασφαλή λειτουργία των δικτύων διαδικτυακών επικοινωνιών.

ΚΕΦΑΛΑΙΟ ΙΙ
Πολιτική Ασφάλειας Παρόχου

Άρθρο 3
Περιεχόμενο Πολιτικής Ασφάλειας

1. Πρωταρχικό στοιχείο για τη διασφάλιση του απορρήτου των επικοινωνιών στο Διαδίκτυο αποτελεί η ύπαρξη στους παρόχους πολιτικής ασφάλειας, η οποία αφορά στους χρήστες, στους χρήστες του παρόχου και στα συστήματα που εμπλέκονται στην επικοινωνία από και προς το Διαδίκτυο.

2. Η πολιτική ασφάλειας παρόχου πρέπει να ανταποκρίνεται στις ειδικές απαιτήσεις ασφάλειας του παρόχου και να καθορίζει την πολιτική πρόσβασης σε συστήματα και πληροφορίες, την πολιτική αποδεκτής χρήσης, τις ενέργειες που ακολουθούνται για τη διατήρηση της ασφάλειας, και τα μέτρα που εφαρμόζονται σε περιπτώσεις παραβίασης της ασφάλειας ή σε έκτακτα γεγονότα.

3. Η πολιτική ασφάλειας διασφαλίζει τα δεδομένα επικοινωνίας των χρηστών και των χρηστών του παρόχου, το απόρρητο των επικοινωνιών, την προστασία των υπολογιστικών συστημάτων και των δικτυακών υποδομών και την προστασία των διαδικτυακών εφαρμογών και υπηρεσιών.

4. Ενδεικτικά, και όχι περιοριστικά, παρατίθενται τα βασικά βήματα που καλείται να ακολουθήσει ο πάροχος προκειμένου να ικανοποιήσει τις απαιτήσεις της πολιτικής ασφάλειας:

(α) εξακρίβωση των στοιχείων που πρέπει να προστατευτούν,

(β) προσδιορισμός των κινδύνων και απειλών για αυτά,

(γ) προσδιορισμός του ρίσκου (πόσο πιθανό είναι να πραγματοποιηθούν οι απειλές),

(δ) υλοποίηση μέτρων προστασίας των στοιχείων με κριτήριο το κόστος υλοποίησης και εφαρμογής,

(ε) συνεχής αναθεώρηση και βελτίωση της πολιτικής ασφάλειας κάθε φορά που ανακαλυφθεί κάποιος κίνδυνος ή κάποια αδυναμία.

5. Μια πολιτική ασφάλειας θεωρείται επαρκής όταν διαθέτει τουλάχιστον τα ακόλουθα χαρακτηριστικά:

(α) Θα πρέπει να είναι πλήρης και αποτελεσματική,

(β) Θα πρέπει να μπορεί να υλοποιηθεί μέσω διαδικασιών διαχείρισης συστημάτων, δημοσιοποίησης οδηγιών αποδεκτής χρήσης ή άλλων αντίστοιχων κατάλληλων μεθόδων. Οι διαδικασίες οι οποίες σχετίζονται με την υλοποίηση της πολιτικής ασφάλειας περιλαμβάνουν τουλάχιστον τη διαπίστωση ταυτότητας (όποτε είναι τεχνικά εφικτό), την εξουσιοδότηση, τον έλεγχο πρόσβασης, την εγκυρότητα, την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα, την τήρηση του απορρήτου, και τον έλεγχο παραβίασης της ασφάλειας,

(γ) Θα πρέπει να μπορεί να εφαρμοστεί μέσω εργαλείων ασφάλειας, ή όταν αυτό δεν είναι εφικτό να καθορίζονται αυστηρές κυρώσεις με αποτρεπτικό χαρακτήρα,

(δ) Θα πρέπει να ορίζει ξεκάθαρα τις περιοχές ευθύνης των χρηστών, των χρηστών του παρόχου και της διοίκησης του παρόχου. Επιπλέον οι μηχανισμοί μεταβολής της πολιτικής ασφάλειας πρέπει να είναι καλά ορισμένοι, περιλαμβάνοντας τη διαδικασία, τους εμπλεκόμενους, καθώς και τους υπεύθυνους προς υπογραφή,

(ε) Θα πρέπει να είναι ανεξάρτητη, στο μέτρο του δυνατού από τεχνικής απόψεως, από το συγκεκριμένο χρησιμοποιούμενο εξοπλισμό (υλικό, λογισμικό),

(στ) Θα πρέπει να είναι βασισμένη σε μια ανοικτή αρχιτεκτονική έτσι ώστε να καθίσταται μακροπρόθεσμα βιώσιμη.

6. Η φύση των επενδύσεων που γίνονται από τους παρόχους για τη διατήρηση της ασφάλειας και της ακεραιότητας των δικτύων τους πρέπει να ακολουθεί την αρχή της αναλογικότητας, η οποία λαμβάνει υπόψη της το μέγεθος του παρόχου σε όρους υποδομής αριθμού χρηστών και αριθμού χρηστών παρόχου.

7. Εφόσον ο πάροχος διαθέτει γενικότερη πολιτική ασφάλειας πληροφοριών και πληροφοριακών συστημάτων (π.χ. η γενικότερη πολιτική ασφάλειας μπορεί να αφορά πρόσβαση σε φυσικούς χώρους όπως κτίρια, δωμάτια, κτλ στα οποία αποθηκεύονται στοιχεία συνδρομητών) τότε θα πρέπει να ενσωματώνει σε αυτήν τη γενικότερη πολιτική και την πολιτική ασφάλειας που αποτελεί αντικείμενο του παρόντος Κανονισμού.

8. Η πολιτική ασφάλειας υπόκειται σε έλεγχο από την ΑΔΑΕ, τόσο ως προς την πληρότητα και αποτελεσματικότητά της, όσο και ως προς τον βαθμό εφαρμογής της.

Άρθρο 4
Περιεχόμενο Πολιτικής Πρόσβασης

1. Η Πολιτική Πρόσβασης (access policy) καθορίζει το επίπεδο πρόσβασης χρηστών και χρηστών παρόχου, καθώς και εργαλείων λογισμικού εποπτείας σε καθένα από τα συστήματα υλικού και λογισμικού από τα οποία αποτελείται ο εξοπλισμός του παρόχου.

2. Η Πολιτική Πρόσβασης αποτελεί αναπόσπαστο τμήμα της Πολιτικής Ασφάλειας.

3. Ο πάροχος οφείλει να διαθέτει και να εφαρμόζει Πολιτική Πρόσβασης για τα συστήματα τα οποία αναφέρονται σε εξωτερικές συνδέσεις, επικοινωνίες δεδομένων, τηλεπικοινωνιακές συσκευές και προγράμματα λογισμικού.

4. Η Πολιτική Πρόσβασης περιγράφει για κάθε σύστημα, με τρόπο λεπτομερή και σαφή, τουλάχιστον τις ακόλουθες διαδικασίες:

(α) Διαδικασίες προσθήκης νέων χρηστών και χρηστών παρόχου στο εν λόγω σύστημα.

(β) Διαδικασίες εξουσιοδότησης (authorization) σχετικά με την προσθήκη, διαγραφή και αλλαγή των επιπέδων πρόσβασης των χρηστών και χρηστών παρόχου σε αρχεία, διαδικασίες λογισμικού και πληροφορίες του εν λόγω συστήματος.

(γ) Διαδικασίες ταυτοποίησης (authentication) χρηστών και χρηστών παρόχου.

(δ) Διαδικασίες ελέγχου των παραπάνω διαδικασιών και διαχείρισης του επιπέδου πρόσβασης που παραχωρείται στους χρήστες και χρήστες παρόχου.

(ε) Διαδικασίες πρόσβασης χρηστών και χρηστών παρόχου σε συστήματα που διατηρούν δεδομένα επικοινωνίας χρηστών .

(στ) Σε περίπτωση που χρησιμοποιείται κρυπτογράφηση, η Πολιτική Πρόσβασης θα πρέπει να περιέχει τις διαδικασίες πρόσβασης χρηστών και χρηστών παρόχου σε συστήματα κρυπτογράφησης / αποκρυπτογράφησης καθώς και σε διαδικασίες σχετικά με την διαχείριση, διανομή, εισαγωγή και αρχειοθέτηση των κλειδιών κρυπτογράφησης. Οι πληροφορίες αυτές θα αναφέρονται σε καταλλήλως διαβαθμισμένο παράρτημα των εγγράφων που περιέχουν την Πολιτική Πρόσβασης.

5. Ειδικότερα, αναφορικά με τη διασφάλιση του απορρήτου των επικοινωνιών:

(α) Ο πάροχος οφείλει να ορίζει τουλάχιστον έναν Υπεύθυνο Πρόσβασης, ο οποίος καθορίζει το είδος της πρόσβασης των χρηστών και των χρηστών παρόχου στα συστήματα.

(β) Ο πάροχος οφείλει να ορίζει τουλάχιστον έναν Υπεύθυνο Συστήματος, ο οποίος υλοποιεί τις αποφάσεις του Υπευθύνου Πρόσβασης.

(γ) Ο πάροχος οφείλει να ορίζει τουλάχιστον έναν Υπεύθυνο Αντιγράφων Ασφάλειας, ο οποίος καθορίζει ποιος έχει πρόσβαση στα αντίγραφα ασφάλειας καθώς και κάθε πότε θα λαμβάνονται αντίγραφα ασφάλειας και για ποια δεδομένα, πάντα σε συνεννόηση με τον Υπεύθυνο Πρόσβασης.

Άρθρο 5
Περιεχόμενο Πολιτικής Αποδεκτής Χρήσης

1. Η Πολιτική Αποδεκτής Χρήσης (Acceptable or Appropriate Use Policy) περιγράφει τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις και δραστηριότητες των χρηστών και των χρηστών παρόχου των υπολογιστικών και τηλεπικοινωνιακών συστημάτων ενός παρόχου.

2. Η Πολιτική Αποδεκτής Χρήσης αποτελεί αναπόσπαστο τμήμα της Πολιτικής Ασφάλειας.

3. Σκοπός της είναι να διασφαλίσει ότι οι χρήστες και οι χρήστες παρόχου δεν θα εκμεταλλευτούν την πρόσβαση που τους παρέχεται σύμφωνα με την Πολιτική Πρόσβασης (Access Policy) σε υπολογιστές, εφαρμογές και παντός είδους τηλεπικοινωνιακά δίκτυα προκειμένου να προβούν σε ενέργειες που παραβιάζουν οποιονδήποτε νόμο του κράτους.

4. Η Πολιτική Αποδεκτής Χρήσης πρέπει να είναι προσαρμοσμένη στην κατηγορία χρηστών στην οποία απευθύνεται και να είναι σύμφωνη με την Πολιτική Πρόσβασης για κάθε κατηγορία χρηστών. Ο πάροχος οφείλει να λαμβάνει υπόψιν κατηγορίες χρηστών όπως χρήστες, χρήστες παρόχου, εργαζόμενοι σε άλλη εταιρεία με την οποία ο πάροχος συνεργάζεται κτλ.

5. Η Πολιτική Αποδεκτής Χρήσης οφείλει να περιλαμβάνει, με όσο το δυνατόν πιο λεπτομερή και κατανοητό τρόπο ώστε να αποφεύγονται οι παρερμηνείες, το ακόλουθο ελάχιστο περιεχόμενο:

(α) Δικαιώματα Χρήστη (ανά κατηγορία χρήστη). Σε αυτήν την ενότητα περιλαμβάνονται μεταξύ άλλων συγκεκριμένα παραδείγματα αποδεκτής χρήσης των συστημάτων στα οποία παρέχεται πρόσβαση βάσει της Πολιτικής Πρόσβασης.

(β) Υποχρεώσεις Χρήστη (ανά κατηγορία χρήστη). Σε αυτή την ενότητα περιλαμβάνονται μεταξύ άλλων συγκεκριμένα παραδείγματα μη αποδεκτής χρήσης των συστημάτων στα οποία παρέχεται πρόσβαση βάσει της Πολιτικής Πρόσβασης, καθώς και συνέπειες μη συμμόρφωσης με αυτές τις υποχρεώσεις.

(γ) Δικαιώματα του παρόχου.

(δ) Υποχρεώσεις του παρόχου.

6. Επιπλέον στην ενότητα που αναφέρεται στις υποχρεώσεις των χρηστών, η Πολιτική Αποδεκτής Χρήσης οφείλει να περιλαμβάνει τις παρακάτω διατάξεις οι οποίες σχετίζονται με την ασφάλεια του συστήματος:

(α) Οι χρήστες και οι χρήστες παρόχου οφείλουν να λαμβάνουν όλα τα ενδεικνυόμενα μέτρα για την διασφάλιση του απορρήτου επικοινωνιών τους, όπως απόκρυψη των μυστικών κωδικών τους (π.χ. passwords), κλείδωμα του ηλεκτρονικού υπολογιστή όταν απομακρύνονται κτλ.

(β) Οι χρήστες και οι χρήστες παρόχου οφείλουν να ενημερώνουν αμέσως τους υπευθύνους του παρόχου αν υποπέσει στην αντίληψή τους οποιοδήποτε κενό ασφάλειας συστήματος που θέτει σε κίνδυνο το απόρρητο επικοινωνιών των ίδιων ή άλλων χρηστών και χρηστών παρόχου.

(γ) Οι χρήστες και οι χρήστες παρόχου οφείλουν να αποκτούν πρόσβαση αποκλειστικά και μόνο σε δεδομένα επικοινωνίας τα οποία αναφέρονται στους ίδιους ή είναι δημοσίως ανακοινώσιμα σύμφωνα με τους κανόνες χειρισμού δεδομένων επικοινωνίας ή για τα οποία τους έχει δοθεί πρόσβαση σύμφωνα με την Πολιτική Πρόσβασης.

(δ) Οι χρήστες και οι χρήστες παρόχου απαγορεύεται να επιχειρούν να εκμεταλλευτούν πιθανά κενά ασφάλειας των συστημάτων του παρόχου προκειμένου να αποκτήσουν πρόσβαση σε πληροφορίες άλλων χρηστών και χρηστών παρόχου, να διαταράξουν την ομαλή λειτουργία των δικτύων, να εκτελέσουν κακόβουλο λογισμικό και γενικά να υποβαθμίσουν το επίπεδο ασφάλειας του συστήματος.

7. Ειδικά σε σχέση με το τηλεπικοινωνιακό απόρρητο, ο πάροχος οφείλει να συμμορφώνεται με τις διατάξεις του Κεφαλαίου ΙΙΙ του παρόντος Κανονισμού.

8. Ο πάροχος οφείλει να δίνει στο χρήστη (ή στο χρήστη παρόχου) πρόσβαση στα συστήματά του μόνο εφόσον ο χρήστης (ή ο χρήστης παρόχου αντίστοιχα) έχει λάβει γνώση και ακολούθως έχει αποδεχθεί την Πολιτική Αποδεκτής Χρήσης. Το γεγονός αυτό αποδεικνύεται είτε με έγγραφη δήλωση του χρήστη (ή του χρήστη παρόχου αντίστοιχα) η οποία φέρει την πρωτότυπη υπογραφή του ή εφόσον ο χρήστης (ή του χρήστη παρόχου αντίστοιχα) έχει συμπληρώσει το αντίστοιχο πεδίο σε σχετική φόρμα αποδοχής στην περίπτωση που η Πολιτική Αποδεκτής Χρήσης παρουσιάζεται ηλεκτρονικά.

9. Ειδικά οι χρήστες παρόχου:

(α) Οφείλουν να συμμορφώνονται με τις διατάξεις των κεφαλαίων ΙΙ και ΙΙΙ του παρόντος σχετικά με την ακρόαση, υποκλοπή, παρακολούθηση, αποθήκευση, επεξεργασία, εξαγωγή, διαβίβαση, ανακοίνωση και δημοσιοποίηση δεδομένων επικοινωνίας, έτσι ώστε να διασφαλίζεται το απόρρητο επικοινωνιών των χρηστών.

(β) Οφείλουν να ακολουθούν τις διαδικασίες δημιουργίας αντιγράφων ασφάλειας δεδομένων σύμφωνα με την Πολιτική Πρόσβασης.

ΚΕΦΑΛΑΙΟ ΙΙΙ
Απόρρητο - Προστασία Επεξεργασίας Δεδομένων Επικοινωνίας

Άρθρο 6
Απόρρητο

1. Το απόρρητο των επικοινωνιών οι οποίες διενεργούνται μέσω δημόσιων δικτύων επικοινωνιών κατοχυρώνεται μέσω της εθνικής και ευρωπαϊκής νομοθεσίας. Οι επικοινωνίες αυτές καλύπτουν τις πληροφορίες και τα δεδομένα τα οποία διακινούνται πάνω από δημόσια δίκτυα επικοινωνιών και εξυπηρετούνται από τις αντίστοιχες υπηρεσίες επικοινωνιών. Συγκεκριμένα, απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των πληροφοριών και δεδομένων από πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των ενδιαφερομένων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια.

2. Η παράγραφος 1 δεν επηρεάζει οποιαδήποτε επιτρεπόμενη από το νόμο καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης ή/και θέσης όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής, όπως για παράδειγμα αποτελεί η παροχή αποδεικτικών στοιχείων μιας εμπορικής συναλλαγής.

3. Η χρήση των δικτύων επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες τόσο στον τερματικό εξοπλισμό χρήστη όσο και στον εξοπλισμό που χρησιμοποιείται για την εξυπηρέτηση της επικοινωνίας επιτρέπεται μόνον εάν παρέχονται στο χρήστη σαφείς πληροφορίες για το σκοπό της επεξεργασίας, και πάντα με την συγκατάθεση αυτού. Αυτό βέβαια δεν ισχύει στην περίπτωση που οι ενέργειες αυτές γίνονται για την εξυπηρέτηση της υπηρεσίας που έχει ρητά ζητήσει ο χρήστης.

4. Τα συστήματα για την παροχή ηλεκτρονικών επικοινωνιακών δικτύων και υπηρεσιών θα πρέπει να σχεδιάζονται έτσι ώστε να περιορίζουν την ποσότητα των απαιτούμενων δεδομένων επικοινωνίας στο ελάχιστο δυνατό. Όσες δραστηριότητες σχετικές με την παροχή υπηρεσίας ηλεκτρονικών επικοινωνιών υπερβαίνουν τη μετάδοση μιας επικοινωνίας και τη χρέωσή της θα πρέπει να βασίζονται σε ομαδοποιημένα δεδομένα κυκλοφορίας, που να μην μπορούν να συσχετίζονται με χρήστες. Όταν αυτό δεν είναι δυνατό, θα πρέπει να θεωρούνται ως υπηρεσίες προστιθέμενης αξίας, για τις οποίες απαιτείται η συγκατάθεση του χρήστη.

5. Οι πάροχοι θα πρέπει να ενημερώνουν τους χρήστες σχετικά με τα μέτρα προστασίας που μπορούν να λαμβάνουν για τη διασφάλιση του απορρήτου των επικοινωνιών και των δεδομένων επικοινωνίας τους, για παράδειγμα τη χρήση συγκεκριμένου τύπου λογισμικού ή τεχνολογιών κρυπτογράφησης.

6. Για τη συλλογή των πληροφοριών από τους χρήστες, θα πρέπει να ισχύει η αρχή της διαφάνειας. Ο πάροχος οφείλει να ενημερώνει τους χρήστες χρησιμοποιώντας κάθε πρόσφορο μέσο αναφορικά με το σκοπό συλλογής των πληροφοριών καθώς και με τους πιθανούς τρόπους επεξεργασίας ή χρήσης τους. Ως εκ τούτου, ο πάροχος οφείλει να προτιμά τους άμεσους τρόπους συλλογής πληροφοριών όπως π.χ. η χρήση ηλεκτρονικών φορμών. Επιπλέον ο πάροχος οφείλει να ενημερώνει τους χρήστες και να εξασφαλίζει τη συγκατάθεσή τους αναφορικά με τις περιπτώσεις που για διάφορους λόγους (ενδεικτικά αναφέρονται λόγοι λειτουργικότητας των διαδικτυακών εφαρμογών) πρέπει να λάβει χώρα έμμεση συλλογή πληροφορίας (π.χ. μέσω cookies).

7. Ο πάροχος οφείλει να ενημερώνει τους χρήστες για τα δεδομένα επικοινωνίας τα οποία πιθανόν αποθηκεύονται σε αντίγραφα ασφάλειας και τα οποία είναι ανακτήσιμα ακόμα και μετά τη διαγραφή τους από το χρήστη. Ο πάροχος οφείλει να κοινοποιεί στους χρήστες το μέγιστο χρονικό διάστημα για το οποίο τα δεδομένα επικοινωνίας είναι αποθηκευμένα στα αντίγραφα ασφάλειας.

8. Από τις διατάξεις του παρόντος άρθρου εξαιρείται η τεχνική αποθήκευση ή αντιγραφή της πληροφορίας, η οποία είναι απολύτως αναγκαία για τη διαβίβαση επικοινωνίας και την εξυπηρέτηση των υπηρεσιών επικοινωνιών. Ενδεικτικά, και όχι περιοριστικά, αναφέρονται εδώ πληροφορίες σε σχέση με την ταυτότητα των χρηστών οι οποίες είναι απαραίτητες για τη δρομολόγηση ή τη χρέωση της κλήσης, η αποθήκευση διευθύνσεων IP σε προσωρινή (cache) μνήμη μέσα στο σύστημα ονοματοθεσίας τομέων (DNS), η αποθήκευση της αντιστοίχισης διευθύνσεων IP σε υλικές διευθύνσεις (MAC addresses) και η χρήση των παρεχόμενων κατά τη σύνδεση (log-in) πληροφοριών για τον έλεγχο του δικαιώματος πρόσβασης σε δίκτυα ή υπηρεσίες.

9. Από τις διατάξεις του παρόντος άρθρου εξαιρείται η τεχνική αποθήκευση ή αντιγραφή ή επεξεργασία της πληροφορίας για σκοπούς διερεύνησης αξιόποινων πράξεων και για σκοπούς προστασίας της εθνικής ασφάλειας και της δημοσίας τάξεως όπως κάθε φορά ορίζεται από την κείμενη νομοθεσία.

Άρθρο 7
Προστασία επεξεργασίας των δεδομένων επικοινωνίας

1. Οι πάροχοι οφείλουν να λαμβάνουν υπόψη και να εφαρμόζουν στο τμήμα της πολιτικής τους τις διατάξεις της κείμενης νομοθεσίας για την προστασία της επεξεργασίας των δεδομένων επικοινωνίας.

Άρθρο 8
Προστασία Επεξεργασίας Αρχείων

1. Σε περιπτώσεις παραβίασης των διατάξεων προστασίας του απορρήτου των επικοινωνιών, οι οποίες περιλαμβάνουν και επεξεργασία αρχείων αρμοδιότητας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η ΑΔΑΕ θα ενημερώνει την εν λόγω Αρχή σχετικά, προκειμένου να επιλαμβάνεται στο πλαίσιο των δικών της αρμοδιοτήτων.

ΚΕΦΑΛΑΙΟ IV -
Υποχρεώσεις Παρόχων - Έλεγχος και Εποπτεία

Άρθρο 9
Υποχρεώσεις Παρόχων αναφορικά
με την Πολιτική Ασφάλειας

1. Όλοι οι πάροχοι υποχρεούνται:

(α) Να διαθέτουν ανά πάσα στιγμή καθορισμένη Πολιτική Ασφάλειας για τη διασφάλιση του απορρήτου διαδικτυακών επικοινωνιών.

(β) Να εφαρμόζουν την εν λόγω πολιτική.

2. Η Πολιτική Ασφάλειας περιέχει όλα όσα καθορίζονται στον παρόντα Κανονισμό, καθώς επίσης και στον «Κανονισμό για τη Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου» και στον «Κανονισμό για τη Διασφάλιση του Απορρήτου Διαδικτυακών Υποδομών».

3. Ο πάροχος οφείλει να προβλέπει στο οργανόγραμμά του διοικητική οντότητα η οποία θα είναι επιφορτισμένη με την κατάρτιση και την εφαρμογή της Πολιτικής Ασφάλειας με επικεφαλής κατάλληλα καταρτισμένο στέλεχος του παρόχου που θα φέρει τον τίτλο του Υπευθύνου Ασφάλειας.

4. Οι πάροχοι οφείλουν να προβαίνουν σε τακτικές επισκοπήσεις και αναθεωρήσεις της πολιτικής ασφάλειας, είτε αυτόβουλα (μετά από έγκριση της ΑΔΑΕ σε περίπτωση αναθεώρησης) είτε ύστερα από σχετική εντολή της ΑΔΑΕ όπως μπορεί να προκύψει από πιθανή διαδικασία ελέγχου ή έκδοση σχετικής οδηγίας.

5. Σε περίπτωση παραβίασης (ή ιδιαίτερου κινδύνου παραβίασης) της πολιτικής ασφάλειας, ιδιαίτερα στην περίπτωση που δεν είναι δυνατό να αντιμετωπιστεί με τα υπάρχοντα μέσα του παρόχου, ο πάροχος οφείλει να ενημερώνει άμεσα τους χρήστες και τους χρήστες παρόχου σχετικά με τους υφιστάμενους κινδύνους ασφάλειας και τις συνέπειες αυτών (συμπεριλαμβανομένου του πιθανού κόστους) και, εάν είναι εφικτό, να παρέχει στοιχεία για την αποτροπή ή αντιμετώπισή τους. Σε κάθε τέτοια περίπτωση οφείλει να ενημερώνει άμεσα την ΑΔΑΕ.

6. Οι πάροχοι οφείλουν να ενημερώνουν τους χρήστες και τους χρήστες παρόχου για την ύπαρξη και τον τρόπο χρήσης πόρων σχετικών με την ασφάλεια των μεταδιδόμενων πληροφοριών (π.χ. Secure Shell Server, SSH)

7. Ο πάροχος οφείλει να ορίζει συνέπειες προς τους χρήστες και τους χρήστες παρόχου σε περίπτωση μη συμμόρφωσής τους με τα προβλεπόμενα από την Πολιτική Ασφάλειας (συμπεριλαμβανομένων των Πολιτικών Πρόσβασης και Αποδεκτής χρήσης)

Άρθρο 10
Διαδικασία Έλεγχου από την ΑΔΑΕ

1. Η ΑΔΑΕ σε τακτά χρονικά διαστήματα διενεργεί έλεγχο σε κάθε πάροχο που εμπίπτει στις διατάξεις του παρόντος. Η συχνότητα των ελέγχων θα καθοριστεί από την ΑΔΑΕ με μεταγενέστερη απόφασή της.

2. Η διαδικασία ελέγχου διενεργείται από τις αρμόδιες υπηρεσίες της ΑΔΑΕ ή από ειδικούς που τελούν υπό την άμεση επίβλεψη της ΑΔΑΕ με βάση τα βήματα που περιγράφονται στο Παράρτημα Α του παρόντος Κανονισμού.

3. Κατά τη διάρκεια του ελέγχου, η ομάδα ελέγχου της ΑΔΑΕ καταγράφει αναλυτικά τις ενέργειες στις οποίες προβαίνει σε ειδικό έντυπο με τίτλο «Έκθεση Διενέργειας Ελέγχου σε Πάροχο Διαδικτυακών Επικοινωνιών αναφορικά με την Πολιτική Ασφάλειας και τη Διασφάλιση του Απορρήτου». Τα ελάχιστα απαραίτητα στοιχεία του εν λόγω εντύπου παρατίθενται στο Παράρτημα Β του παρόντος Κανονισμού.

4. Η ομάδα ελέγχου κοινοποιεί το πόρισμα της στην Ολομέλεια της ΑΔΑΕ. Η Ολομέλεια της ΑΔΑΕ αξιολογεί τα ευρήματα του ελέγχου και είτε εγκρίνει τις ενέργειες που προβλέπονται στην εκάστοτε πολιτική ασφάλειας του παρόχου που έχει εγκριθεί από την ΑΔΑΕ είτε επιβάλλει κυρώσεις εφόσον δεν έχουν ληφθεί τα προσήκοντα μέτρα.

5. Ως προς τη διαδικασία και τις κυρώσεις της παραγρ. 4 ισχύουν οι διατάξεις του Ν.3115/2003 άρθρο 11 και 6 παρ. 4, καθώς και τα προβλεπόμενα στον εσωτερικό κανονισμό της ΑΔΑΕ (ΦΕΚ 1642/Β/7-11-2003).

Άρθρο 11
Άσκηση Εποπτείας

1. Κάθε πάροχος στο τέλος του ημερολογιακού έτους υποβάλλει στην ΑΔΑΕ ετήσια έκθεση με στοιχεία που αφορούν στην ασφάλεια των διαδικτυακών επικοινωνιών και τη διασφάλιση του απορρήτου.

2. Το ελάχιστο περιεχόμενο της ετήσιας έκθεσης ορίζεται ως εξής:

(α) Περιστατικά που απείλησαν την ασφάλεια του παρόχου και τη διασφάλιση του απορρήτου καθώς και τυχόν βλάβες που υπέστη ο πάροχος, οι χρήστες του και οι χρήστες παρόχου εξαιτίας αυτών.

(β) Μέτρα που ελήφθησαν για την αντιμετώπιση των ως άνω περιστατικών.

3. Η ΑΔΑΕ με Απόφασή της δύναται να μεταβάλλει το ελάχιστο περιεχόμενο της ετήσιας έκθεσης.

4. Η ΑΔΑΕ δύναται να ζητήσει εκτάκτως από τους παρόχους οποιεσδήποτε πληροφορίες θεωρεί αναγκαίες στα πλαίσια των αρμοδιοτήτων της για την ασφάλεια των διαδικτυακών επικοινωνιών και τη διασφάλιση του απορρήτου.

ΚΕΦΑΛΑΙΟ V - ΜΕΤΑΒΑΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 12
Μεταβατικές Διατάξεις

1. Όλοι οι πάροχοι υποχρεούνται:

(α) Να ενημερώσουν ως προς την εφαρμοζόμενη πολιτική ασφάλειας την ΑΔΑΕ εντός έξι (6) μηνών από τη δημοσίευση του παρόντος.

(β) Να εφαρμόζουν την εγκριθείσα από την ΑΔΑΕ πολιτική ασφάλειας εντός ενός (1) έτους από την έγκρισή της.

ΚΕΦΑΛΑΙΟ VI - ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 13
Έναρξη Ισχύος

1. Ο παρών Κανονισμός τίθεται σε ισχύ από την ημερομηνία δημοσίευσής του στην Εφημερίδα της Κυβερνήσεως.

ΠΑΡΑΡΤΗΜΑ Α

Αναλυτική περιγραφή διαδικασίας ελέγχου παρόχου

Η διαδικασία ελέγχου παρόχου διενεργείται με βάση τα ακόλουθα βήματα:

(α) Η ΑΔΑΕ με Απόφασή της ορίζει ομάδα ελέγχου που αποτελείται από τρία (3) τουλάχιστον άτομα με σκοπό τον έλεγχο συγκεκριμένου παρόχου. Η ελάχιστη στελέχωση της ομάδας ελέγχου περιλαμβάνει έναν (1) υπεύθυνο της ομάδας, ένα (1) νομικό σύμβουλο και έναν (1) τεχνικό σύμβουλο.

(β) Σε χρόνο που αποφασίζει η ομάδα ελέγχου, επικοινωνεί με τον πάροχο και ζητεί να έρθει σε άμεση επικοινωνία με τον υπεύθυνο ασφάλειας όπως αυτός ορίζεται στο Άρθρο 6 του παρόντος. Τυχόν καθυστέρηση ή κώλυμα που παρουσιάζεται κατά την προσπάθεια επικοινωνίας με τον υπεύθυνο ασφάλειας καταγράφεται και φέρει τις ανάλογες κυρώσεις.

(γ) Ο υπεύθυνος ασφάλειας παραδίδει στην ομάδα ελέγχου πλήρες αντίγραφο της πολιτικής ασφάλειας (συμπεριλαμβανομένης της πολιτικής πρόσβασης και της πολιτικής αποδεκτής χρήσης) και των τυχών συνοδευτικών εγγράφων. Από τα παραδιδόμενα έγγραφα θα πρέπει να προκύπτουν οι ημερομηνίες έκδοσης και έγκρισης των συγκεκριμένων πολιτικών. Τυχόν καθυστέρηση επίδοσης σημειώνεται και φέρει τις ανάλογες κυρώσεις.

(δ) Η ομάδα ελέγχου προβαίνει σε αναλυτική εξέταση όλων των σχετικών εγγράφων και καταγράφονται οι τυχόν ελλείψεις που παρουσιάζονται στην πολιτική ασφάλειας του παρόχου. Κατά την διαδικασία αυτή δύναται να ζητηθεί η συνδρομή του παρόχου έτσι ώστε να διασαφηνιστούν τυχόν ασάφειες και προβλήματα που παρουσιάζονται στην πολιτική ασφάλειας.

(ε) Κατά τη διάρκεια του ελέγχου ο πάροχος δεν έχει την δυνατότητα να αντικαταστήσει την πολιτική ασφάλειας με νέα ούτε να προβεί σε τυχόν διορθώσεις αυτής.

(στ) Τυχόν ασάφειες στην Πολιτική Ασφάλειας θεωρούνται ως σφάλματα, μιας και η πολιτική αυτή θα πρέπει να έχει διατυπωθεί κατά τρόπο σαφή.

(ζ) Η ομάδα ελέγχου προβαίνει σε αυτοψία των εγκαταστάσεων του παρόχου για να διαπιστώσει σε ποιο βαθμό εφαρμόζονται οι διαδικασίες που προβλέπονται από τα προσκομιθέντα έγγραφα. Η αυτοψία δύναται να περιλαμβάνει και επαφή με το προσωπικό του παρόχου. Η ομάδα ελέγχου καταγράφει αναλυτικά τις ελλείψεις και τα σφάλματα που τυχόν διαπιστωθούν.

(η) Ο πάροχος οφείλει να υποβάλει στην ομάδα ελέγχου οποιοδήποτε στοιχείο θεωρηθεί απαραίτητο από την ομάδα για την επιτυχή ολοκλήρωση του ελέγχου.

(θ) Τυχόν διαπίστωση έλλειψης συνεργασίας από τον πάροχο ή/και προσπάθειας παραπλάνησης της ομάδας ελέγχου καταγράφεται και φέρει τις ανάλογες κυρώσεις.

ΠΑΡΑΡΤΗΜΑ Β

Ελάχιστο περιεχόμενο του εντύπου με τίτλο

«Έκθεση Διενέργειας Ελέγχου σε Πάροχο Διαδικτυακών Επικοινωνιών αναφορικά με την Πολιτική Ασφάλειας και τη Διασφάλιση του Απορρήτου»

Το ως άνω έντυπο θα περιέχει απαραιτήτως τουλάχιστον τα ακόλουθα στοιχεία:

(α) Τα στοιχεία της Απόφασης της ΑΔΑΕ με την οποία αποφασίστηκε ο έλεγχος.

(β) Τα ονοματεπώνυμα και τις ιδιότητες των στελεχών της ΑΔΑΕ που απαρτίζουν την ομάδα ελέγχου καθώς και την ημερομηνία σύστασής της.

(γ) Το όνομα του υπό έλεγχο παρόχου καθώς και το όνομα του υπευθύνου ασφάλειάς του.

(δ) Το χρόνο που απαιτήθηκε έως ότου να αποδοθεί στην ομάδα ελέγχου η πλήρης Πολιτική Ασφάλειας του παρόχου.

(ε) Ημερολόγιο ενεργειών και ερωτήσεων της ομάδας ελέγχου και καταγραφή της ανταπόκρισης του ελεγχόμενου παρόχου.

(στ) Το αποτέλεσμα της αυτοψίας για την αποτίμηση της εφαρμογής της Πολιτικής Ασφάλειας με καταγραφή τυχόν ελλείψεων και ασαφειών.

(ζ) Τις ημερομηνίες έναρξης και περάτωσης του ελέγχου.

(η) Το τελικό πόρισμα του ελέγχου και την εισήγηση προς την Ολομέλεια της ΑΔΑΕ.

Ο παρών Κανονισμός να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Αθήνα, 14 Ιανουαρίου 2005

Ο Πρόεδρος
ΑΝΔΡΕΑΣ ΛΑΜΠΡΙΝΟΠΟΥΛΟΣ

Αριθ. 633 α (2)

Κανονισμός για τη Διασφάλιση του Απορρήτου Διαδικτυακών Υποδομών.

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΑΔΕΑ)

Έχοντας υπόψη:

α. Το Ν. 3115/27.2.2003, άρθρο 1, παραγρ. 1,

β. Το Ν. 3115/27.2.2003, άρθρο 6, παραγρ. 1,

γ. Ότι εκ της αποφάσεως δεν προκύπτει δαπάνη για το δημόσιο

δ. Τη σχετική εισήγηση της Υπηρεσίας, αποφάσισε

Κατά τη συνεδρίασή της την 10η Νοεμβρίου 2004 , την έγκριση του παρακάτω Κανονισμού για τη Διασφάλιση του Απορρήτου Διαδικτυακών Υποδομών.

ΚΕΦΑΛΑΙΟ Ι
ΣΚΟΠΟΣ - ΟΡΙΣΜΟΙ

Άρθρο 1
Σκοπός - Πεδίο Εφαρμογής

1. Σκοπός του παρόντος Κανονισμού είναι:

(α) Η ασφάλεια των Διαδικτυακών υποδομών των παρόχων και η διασφάλιση του απορρήτου αυτών.

(β) Η θέσπιση των υποχρεώσεων των εν λόγω παρόχων αναφορικά με την ασφάλεια και το απόρρητο των Διαδικτυακών τους υποδομών.

(γ) Ο έλεγχος στους εν λόγω παρόχους σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

2. Στις διατάξεις του παρόντος Κανονισμού εμπίπτουν όλοι οι Τηλεπικοινωνιακοί Πάροχοι Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα:

(α) Πάροχοι σταθερής και κινητής πρόσβασης στο Διαδίκτυο,

(β) Πάροχοι Διαδικτυακών υπηρεσιών, υπηρεσιών προστιθέμενης αξίας και υπηρεσιών εφαρμογών.

3. Ο παρών Κανονισμός συμπληρώνει τον «Κανονισμό για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές» καθώς και τον «Κανονισμό για τη Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου» που προηγήθηκαν .

Άρθρο 2
Ορισμοί

Για την εφαρμογή του παρόντος Κανονισμού ισχύουν οι ορισμοί των προαναφερθέντων Κανονισμών της ΑΔΑΕ, που επαναλαμβάνονται εδώ για λόγους πληρότητας. Επιπρόσθετα, οι ακόλουθοι όροι έχουν την έννοια που τους αποδίδεται κατωτέρω:

Αντίγραφα ασφαλείας - Τα εφεδρικά αντίγραφα που προκύπτουν μετά την εφαρμογή των κατάλληλων μεθόδων αντιγραφής και σχετίζονται με τα δεδομένα διάρθρωσης των δικτυακών στοιχείων.

Απειλή (Threat) - Κάθε άτομο, δραστηριότητα ή συμβάν που είναι δυνατόν να προκαλέσει παραβίαση της διαθεσιμότητας, ακεραιότητας ή εμπιστευτικότητας σε οποιοδήποτε σύστημα το οποίο χρησιμοποιείται για την παρακολούθηση, αποθήκευση, επεξεργασία, εξαγωγή, διαβίβαση, ανακοίνωση και δημοσιοποίηση δεδομένων επικοινωνίας. Οι απειλές μπορεί να είναι τυχαίες ή σκόπιμες και μπορεί να προέρχονται είτε από το εσωτερικό είτε από το εξωτερικό του παρόχου.

Αποστρατιωτικοποιημένη Ζώνη (Demilitarized Zone) - Το υποδίκτυο του παρόχου που βρίσκεται μεταξύ των εξωτερικών δικτύων (π.χ. το Διαδίκτυο) και του έμπιστου εσωτερικού δικτύου του παρόχου. Τυπικά σε αυτή τη ζώνη τοποθετούνται συστήματα που παρέχουν υπηρεσίες προσβάσιμες από οποιονδήποτε μέσω του Διαδικτύου ή άλλων εξωτερικών δικτύων (π.χ. διακομιστές παγκόσμιου ιστού και ηλεκτρονικού ταχυδρομείου).

Ασύμμετρη Κρυπτογραφία - Κρυπτογραφία που στηρίζεται στη χρήση ενός ζευγαριού κλειδιών, ενός ιδιωτικού και ενός δημόσιου. Όταν η κρυπτογράφηση γίνεται με το ένα κλειδί, η αποκρυπτογράφηση γίνεται με το άλλο. Είναι γνωστή και ως Κρυπτογραφία Δημόσιου Κλειδιού.

Ακεραιότητα - Ιδιότητα της διαδικασίας ασφάλειας, με την οποία ελέγχεται αν τα δεδομένα έχουν τροποποιηθεί ή καταστραφεί κατά μη εξουσιοδοτημένο τρόπο.

Αυξητική Αντιγραφή (incremental backup) - Αντιγραφή μόνο των αρχείων τα οποία έχουν προστεθεί ή τροποποιηθεί πρόσφατα. Εξυπηρετεί την επιτάχυνση της διαδικασίας αντιγραφής αφού αποθηκεύονται μόνο τα αρχεία που έχουν αλλάξει μετά από την εκτέλεση της τελευταίας αντιγραφής.

Δεδομένα Διάρθρωσης (configuration data) - Τα απαραίτητα στοιχεία δεδομένων που σχετίζονται με τη διάρθρωση, τον προγραμματισμό και τη σωστή λειτουργία των δικτυακών διατάξεων του παρόχου.

Δεδομένα Θέσης - Τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.

Δεδομένα Κίνησης - Τα δεδομένα που υποβάλλονται σε επεξεργασία με σκοπό τη διαβίβαση μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της.

Διαδικτυακές Επικοινωνίες - Υπηρεσίες ηλεκτρονικών επικοινωνιών οι οποίες παρέχονται από δίκτυο μετάδοσης δεδομένων και φωνής με πακετομεταγωγή το οποίο είτε έχει τη μορφή ενδοδικτύου (Intranet) είτε είναι ολόκληρο το Διαδίκτυο (Internet).

Διακομιστής (server) - Πληροφοριακό σύστημα το οποίο παρέχει δεδομένα και υπηρεσίες σε άλλα υπολογιστικά συστήματα, γνωστά ως πελάτες (clients), τα οποία συνδέονται σε αυτόν από απόσταση και με δική τους πρωτοβουλία.

Διαμόρφωση ή Διάρθρωση (configuration) - Διαδικασία κατά την οποία αρχικοποιούνται ή μεταβάλλονται τα δεδομένα διάρθρωσης.

Διαφορική Αντιγραφή (differential backup) - Αντιγραφή που αποθηκεύει όλα τα αρχεία που έχουν αλλάξει από την τελευταία πλήρη αντιγραφή. Δεν αποθηκεύει τα αρχεία της τελευταίας πλήρους αντιγραφής.

Δικτυακή Σύνοδος (session) - Η ακολουθία αλληλεπιδράσεων μεταξύ δύο άκρων επικοινωνίας που λαμβάνει χώρα κατά τη διάρκεια μιας δικτυακής επικοινωνίας.

Δικτυακοί Πόροι - Τα συστήματα (υπολογιστές, εξυπηρετητές, δικτυακοί κόμβοι, κ.α.) που απαρτίζουν το δίκτυο του παρόχου ή είναι συνδεδεμένα σε αυτό, αλλά και τα δεδομένα που αποθηκεύονται και διακινούνται καθώς και οι υπηρεσίες που προσφέρονται από το δίκτυο του παρόχου.

Δίκτυο Ηλεκτρονικών Επικοινωνιών - Τα συστήματα μετάδοσης και, κατά περίπτωση, ο εξοπλισμός μεταγωγής ή δρομολόγησης και οι λοιποί πόροι που επιτρέπουν τη μεταφορά σημάτων, με τη χρήση καλωδίου, ραδιοσημάτων, οπτικού ή άλλου ηλεκτρομαγνητικού μέσου, συμπεριλαμβανομένων των δορυφορικών δικτύων, των σταθερών (μεταγωγής δεδομένων μέσω κυκλωμάτων και πακετομεταγωγής, συμπεριλαμβανομένου του Διαδικτύου) και κινητών επίγειων δικτύων, των συστημάτων ηλεκτρικών καλωδίων, εφόσον χρησιμοποιούνται για τη μετάδοση σημάτων, των δικτύων που χρησιμοποιούνται για ραδιοτηλεοπτικές εκπομπές, καθώς και των δικτύων καλωδιακής τηλεόρασης, ανεξάρτητα από το είδος των μεταφερόμενων πληροφοριών.

Δοκιμαστικά Δεδομένα - Δεδομένα που απαιτούνται από τον τηλεπικοινωνιακό εξοπλισμό του παρόχου για την παροχή υπηρεσιών (ενδεικτικά αναφέρονται ονόματα χρήστη, αριθμοί κλήσης κλπ.) και τα οποία είτε δεν αντιστοιχούν σε χρήστες είτε αντιστοιχούν σε στελέχη ή / και χρήστες του οργανισμού οι οποίοι εν γνώσει τους συμμετέχουν σε δοκιμές τηλεπικοινωνιακού εξοπλισμού (φιλικοί χρήστες).

Δοκιμές Αποδοχής - Διαδικασία εκτέλεσης δοκιμών της λειτουργίας ενός προϊόντος ή υπηρεσίας, μέσω της οποίας ελέγχεται κατά πόσον το προϊόν συμμορφώνεται αφενός με την περιγραφή του κατασκευαστή και αφετέρου με τις απαιτήσεις του αγοραστή.

Δρομολογητής (router) - Τηλεπικοινωνιακός εξοπλισμός που παρέχει υπηρεσίες δρομολόγησης δεδομένων στο στρώμα δικτύου με βάση τη στοίβα πρωτοκόλλων του Διαδικτύου.

Εμπιστευτικότητα - Η ιδιότητα της διαδικασίας ασφάλειας με την οποία αποτρέπεται η διάθεση ή η αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένα άτομα, οντότητες ή διεργασίες.

Εξουσιοδότηση - Η διαδικασία χορήγησης δικαιώματος πρόσβασης ή χρήσης μιας υπηρεσίας ή πληροφοριών, με βάση την έγκυρη ταυτότητα. Η εξουσιοδότηση χορηγείται από την οντότητα που ελέγχει τον πόρο για τον οποίο ζητείται η πρόσβαση.

Επαλήθευση Ταυτότητας (Authentication) - Οι αυτοματοποιημένες και τυποποιημένες μέθοδοι για την πιστοποίηση της ταυτότητας του χρήστη στο Διαδίκτυο. Αναφέρεται και ως αυθεντικοποίηση.

Επισύνδεση ή Εισβολή (Intrusion) - Απόπειρα παραβίασης της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των υπολογιστικών συστημάτων και των δικτύων του παρόχου, καθώς και προσπάθεια παράκαμψης των μηχανισμών ασφάλειας αυτών.

Ευπάθεια (vulnerability) - Αδυναμία ή ελάττωμα στο υλικό (hardware), στο λογισμικό (software) ή στην αρχιτεκτονική ενός συστήματος, καθώς και στις διαδικασίες ασφαλείας που ακολουθούνται, που μπορεί κάποιος να εκμεταλλευτεί προκειμένου να παραβιάσει τη διαθεσιμότητα, ακεραιότητα ή εμπιστευτικότητα του εν λόγω συστήματος.

Θύρα (port) - Άκρο μιας λογικής σύνδεσης του στρώματος μεταφοράς όπως αυτό ορίζεται με βάση τη στοίβα πρωτοκόλλων του Διαδικτύου.

Ιός (virus) - Στοιχείο λογισμικού το οποίο εισβάλλει σε ένα υπολογιστικό σύστημα με σκοπό να προκαλέσει ανεπιθύμητα αποτελέσματα, όπως καταστροφή δεδομένων χρήστη, άρνηση υπηρεσίας (denial-of-service), παραβίαση του συστήματος ασφάλειας κτλ. Κύριο χαρακτηριστικό του είναι το γεγονός ότι μεταδίδεται μεταξύ των υπολογιστικών συστημάτων με τη μορφή εκτελέσιμων προγραμμάτων (executables), εγγραφών συστήματος (system or boot records) και μακρο-εντολών (macros). Οι ιοί είναι δυνατόν να επιτεθούν κατά προσωπικών υπολογιστών, διακομιστών, δρομολογητών κτλ.

Κλειδί Κρυπτογράφησης - Σειρά από bits συγκεκριμένου μήκους που χρησιμοποιείται για να κρυπτογραφήσει ή να αποκρυπτογραφήσει τα δεδομένα σε έναν αλγόριθμο κρυπτογράφησης.

Λογισμικό Ελέγχου - Το λογισμικό το οποίο χρησιμοποιείται για τη διεξαγωγή ελέγχων και μετρήσεων με σκοπό τον έλεγχο ασφάλειας δικτύου.

Λογισμικό Προστασίας από Ιούς (anti-virus software) - Κατηγορία εφαρμογών λογισμικού που αποσκοπεί στην ανίχνευση και απομάκρυνση ιών που έχουν προσβάλλει ένα υπολογιστικό σύστημα.

Μη Αποποίηση Ευθύνης - Διαδικασία που εξασφαλίζει ότι οι συναλλασσόμενοι σε εφαρμογές και υπηρεσίες Διαδικτύου που προσφέρονται είτε από πάροχους διαδικτύου είτε από πάροχους υπηρεσίας εφαρμογής δεν μπορούν να αρνηθούν τη συμμετοχή τους στη συναλλαγή.

Ομάδα Ελέγχου Ασφάλειας Δικτύου - Ομάδα Εργασίας του παρόχου, η οποία πρόκειται να πραγματοποιήσει έλεγχο ασφάλειας δικτύου σε υπολογιστικό και δικτυακό εξοπλισμό.

Παροχή Δικτύου Διαδικτυακών Επικοινωνιών - Η σύσταση, η λειτουργία, ο έλεγχος και η διάθεση τέτοιου δικτύου.

Πάροχος Δικτύου Διαδικτυακών Επικοινωνιών (Internet Service Provider) - Η επιχείρηση ή το νομικό πρόσωπο που παρέχει δίκτυο διαδικτυακών επικοινωνιών ή/και το νομικό πρόσωπο που παρέχει στο προσωπικό του την απαραίτητη δικτυακή υποδομή για χρήση διαδικτυακών επικοινωνιών στα πλαίσια της εργασίας του. Για τις ανάγκες του παρόντος ο πάροχος δικτύου διαδικτυακών επικοινωνιών θα αναφέρεται στη συνέχεια του κειμένου ως «πάροχος διαδικτύου».

Πάροχος Υπηρεσίας Εφαρμογής (Application Service Provider) - μία οντότητα (οργανισμός, εταιρεία κτλ), η οποία διαθέτει εφαρμογές λογισμικού (software), υλική υποδομή (hardware) και δικτυακή υποδομή, προκειμένου να παρέχει υπηρεσίες και εφαρμογές στον πάροχο δικτύου διαδικτυακών επικοινωνιών και τους χρήστες του.

Περιβάλλον Δοκιμής - Τμήμα του εξοπλισμού του παρόχου, το οποίο είναι δικτυακά απομονωμένο από το Περιβάλλον Παραγωγής και χρησιμοποιείται για δοκιμές, εκπαίδευση, παρουσιάσεις κλπ.

Περιβάλλον Παραγωγής - Το σύνολο του εξοπλισμού του παρόχου το οποίο χρησιμοποιείται για ανταλλαγή δεδομένων και παροχή υπηρεσιών στους υπαλλήλους, στους πελάτες και στους συνεργάτες του παρόχου και βρίσκεται συνήθως εντός της περιμέτρου του παρόχου και προστατευόμενο από το εταιρικό firewall.

Περίμετρος Δικτύου - Όλα τα σημεία πρόσβασης του δικτύου του παρόχου σε εξωτερικά δίκτυα (Διαδίκτυο, δίκτυα άλλων υποκαταστημάτων του παρόχου, δίκτυα συνεργατών του, ασύρματα δίκτυα, κτλ)

Πηγαίος Κώδικας - Η μορφή στην οποία βρίσκεται το λογισμικό (συνήθως σε μορφή εντολών κάποιας γλώσσας προγραμματισμού υψηλού επιπέδου κατανοητή στον άνθρωπο) προτού περάσει από διαδικασία μεταγλώττισης και μετατραπεί σε μορφή κατανοητή από το εκάστοτε υπολογιστικό σύστημα.

Πλήρης Αντιγραφή (full backup) - Πλήρης αποθήκευση κάθε αρχείου ενός διακομιστή ή δικτυακού στοιχείου.

Πολιτική Ασφάλειας - Το σύνολο τεχνικών, οργανωτικών και κανονιστικών μέτρων, τα οποία εφαρμόζονται από πάροχο διαδικτύου και αποβλέπουν στη διασφάλιση του απορρήτου και γενικά στην ασφαλή λειτουργία των δικτύων διαδικτυακών επικοινωνιών.

Πόροι Δεδομένων Επικοινωνιών - οι πόροι λογισμικού (software), υλικού (hardware), συστημάτων, υπηρεσιών και δικτύων όπου αποθηκεύονται, επεξεργάζονται, διαβιβάζονται και ανακοινώνονται δεδομένα επικοινωνιών χρηστών.

Προσδιορισμός Ταυτότητας - Αναφέρεται σε λιγότερο τυποποιημένες μεθόδους (σε σχέση με τη διαδικασία επαλήθευσης ταυτότητας) για την πιστοποίηση της φύσης του χρήστη, που είναι συνήθως μη αυτόματες και απαιτούν ανθρώπινη παρέμβαση.

Προστασία του Απορρήτου - Η απαγόρευση της ακρόασης, της παγίδευσης, της αποθήκευσης, της επεξεργασίας, της ανακοίνωσης, της δημοσιοποίησης ή άλλου τύπου υποκλοπής ή παρακολούθησης της τηλεπικοινωνίας και των δεδομένων επικοινωνίας από άλλα πρόσωπα, χωρίς τη συγκατάθεσή τους, εξαιρουμένων των νόμιμα εξουσιοδοτημένων.

Συγκατάθεση του Χρήστη ή του Συνδρομητή - Η συγκατάθεση του προσώπου που αφορούν τα δεδομένα επικοινωνιών, κατά την έννοια της οδηγίας 95/46/ΕΚ.

Συμμετρική Κρυπτογραφία - Κρυπτογραφία στην οποία η κρυπτογράφηση και αποκρυπτογράφηση πραγματοποιούνται με ένα κλειδί.

Σύστημα Ανίχνευσης Επισύνδεσης (Intrusion Detection System) - Το σύστημα που παρακολουθεί τα διάφορα γεγονότα στα υπολογιστικά συστήματα και δίκτυα του παρόχου και τα αναλύει για να εντοπίσει σημάδια επισυνδέσεων.

Ταυτότητα - Οι πληροφορίες που προσδιορίζουν τον χρήστη με μοναδικό τρόπο.

Τοίχος Προστασίας (Firewall) - Το σύστημα που υλοποιείται με λογισμικό ή/και υλικό για την προστασία του εσωτερικού δικτύου του παρόχου από εξωτερικές επιθέσεις.

Υπεργολάβος - Όπως ορίζεται από την ισχύουσα νομοθεσία.

Υπηρεσία Προστιθέμενης Αξίας - Υπηρεσία μη τηλεπικοινωνιακή η οποία μπορεί να παρέχεται ή να υποστηρίζεται από δίκτυο διαδικτυακών επικοινωνιών.

Υπηρεσίες Ηλεκτρονικών Επικοινωνιών - Οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις. Στις υπηρεσίες ηλεκτρονικών επικοινωνιών δεν περιλαμβάνονται υπηρεσίες παροχής ή ελέγχου περιεχόμενου που μεταδίδεται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και υπηρεσίες της κοινωνίας της πληροφορίας, όπως αυτές ορίζονται στην παράγραφο 2 του άρθρου 2 του ΠΔ39/2001 (Α'28), και που δεν αφορούν, εν όλω ή εν μέρει, τη μεταφορά σημάτων σε δίκτυα επικοινωνιών.

Υπολειπόμενος Κίνδυνος (Residual Risk) - Κίνδυνος που εξακολουθεί να υφίσταται ακόμα και μετά την υλοποίηση μέτρων ασφαλείας που αντιμετωπίζουν ένα κίνδυνο παραβίασης του απορρήτου επικοινωνιών των χρηστών.

Χρήστης: κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας.

Χρήστης Παρόχου: κάθε φυσικό πρόσωπο που εργάζεται στην επιχείρηση ή το νομικό πρόσωπο που παρέχει στο προσωπικό του την απαραίτητη δικτυακή υποδομή για χρήση διαδικτυακών επικοινωνιών στα πλαίσια της εργασίας του.

ΚΕΦΑΛΑΙΟ ΙΙ
ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΕΡΙΜΕΤΡΟΥ

Άρθρο 3
Γενικά

1. Ο πρωταρχικός σκοπός της πολιτικής ασφάλειας περιμέτρου είναι να προστατεύσει τους διάφορους δικτυακούς πόρους του παρόχου διαδικτύου από εισβολείς, δηλαδή να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση σε στοιχεία του δικτύου του παρόχου διαδικτύου (σε υλικό ή λογισμικό), καθώς και τη διακοπή της ομαλής παροχής των υπηρεσιών του παρόχου διαδικτύου. Δεδομένου ότι οι κίνδυνοι και οι απειλές της ασφάλειας των δικτυακών πόρων δεν μπορούν να ελεγχθούν εξ ολοκλήρου, σκοπός της πολιτικής ασφάλειας περιμέτρου είναι να διατηρήσει ένα ικανοποιητικό επίπεδο ασφάλειας, ιδιαίτερα όσον αφορά την πρόσβαση από/προς το Διαδίκτυο, ανάλογα με την Αποτίμηση Κινδύνου (Κεφάλαιο VII) που οφείλει πρώτα ο πάροχος διαδικτύου να έχει πραγματοποιήσει.

2. Η πολιτική ασφάλειας περιμέτρου ορίζει τους μηχανισμούς (σε υλικό και λογισμικό) που χρησιμοποιούνται για τον σκοπό που περιγράφηκε παραπάνω, καθώς και τους τρόπους διαμόρφωσης και ανανέωσης αυτών. Ενδεικτικά και όχι περιοριστικά αναφέρονται τα εξής συστήματα: Τοίχος Προστασίας (firewall), Σύστημα Προστασίας Αποστρατιωτικοποιημένης Ζώνης, και Σύστημα Ανίχνευσης Επισυνδέσεων (Intrusion Detection System), μεταξύ άλλων.

3. Προκειμένου η πολιτική ασφάλειας περιμέτρου να εξασφαλίζει το επιθυμητό επίπεδο ασφάλειας των δικτυακών πόρων ενός παρόχου διαδικτύου, πρέπει ο πάροχος διαδικτύου να ακολουθεί τις διεθνώς, ευρέως αποδεκτές πρακτικές που αφορούν την πολιτική ασφάλειας περιμέτρου. Αυτό συνεπάγεται την κατάλληλη επιλογή, διαμόρφωση, και ανανέωση των συστημάτων που υλοποιούν την ασφάλεια περιμέτρου.

4. Ο πάροχος διαδικτύου οφείλει να ορίζει Υπεύθυνο Πολιτικής Ασφάλειας Περιμέτρου, ο οποίος είναι υπεύθυνος για τον καθορισμό της πολιτικής ασφάλειας περιμέτρου και για τη σωστή εφαρμογή της. Για τον σκοπό αυτό, ο πάροχος διαδικτύου οφείλει να αναγνωρίζει ότι η διαχείριση των συστημάτων περιμετρικής ασφάλειας απαιτεί σημαντικό χρόνο και κατάλληλη εκπαίδευση, και να εξασφαλίζει αυτά στον Υπεύθυνο Πολιτικής Ασφάλειας Περιμέτρου.

Άρθρο 4
Συστήματα Firewalls

1. Ο πάροχος διαδικτύου υποχρεούται να χρησιμοποιεί συστήματα firewall για την προστασία των συνδέσεων του δικτύου του με το Διαδίκτυο ή με άλλα δίκτυα, σύμφωνα με την πολιτική ασφάλειας περιμέτρου που έχει ορίσει, χωρίς διακοπή (24 ώρες το 24ωρο). Διακοπή της λειτουργίας των συστημάτων επιτρέπεται σε περιπτώσεις συντήρησης ή αναβάθμισης, ύστερα όμως από έγκαιρη ενημέρωση των χρηστών και αναβολή της συνδεσιμότητας του δικτύου με εξωτερικά δίκτυα και το Διαδίκτυο για όσο χρόνο διαρκούν οι διαδικασίες αυτές.

2. Ο πάροχος διαδικτύου πρέπει ιδιαίτερα να εξασφαλίζει την ασφάλεια των ιδίων συστημάτων firewall, όπως για παράδειγμα μέσω της χρήσης ενός πολύ ασφαλούς λειτουργικού συστήματος για τα συστήματα αυτά.

3. Οι πάροχοι διαδικτύου οφείλουν να αντιμετωπίζουν τα συστήματα firewall ως την πρώτη γραμμή άμυνας από εξωτερικές απειλές, τα οποία όμως δεν διασφαλίζουν πλήρως την ασφάλεια των εσωτερικών συστημάτων, τα οποία πρέπει να προστατεύονται αυτόνομα και διαρκώς.

4. Η αρχιτεκτονική των συστημάτων firewall που θα αναπτυχθεί σε έναν πάροχο διαδικτύου πρέπει να διακρίνει το εσωτερικό δίκτυο σε δύο βασικές περιοχές: (α) εσωτερικό έμπιστο (trusted) δίκτυο και (β) δίκτυο αποστρατικοποιημένης ζώνης. Το σύστημα firewall επιβάλλεται να μην επιτρέπει την απευθείας πρόσβαση σε δεδομένα που υπάρχουν στα πληροφοριακά συστήματα και τα δικτυακά στοιχεία του εσωτερικού έμπιστου δικτύου.

5. Η επιλογή, διαμόρφωση και ανανέωση των συστημάτων firewall γίνεται με βάση τις διεθνώς, ευρέως αποδεκτές πρακτικές, οι οποίες περιλαμβάνουν αλλά δεν περιορίζονται στις εξής:

(α) Η βασική πολιτική διαμόρφωσης ενός firewall σχετικά με την εισερχόμενη κίνηση είναι να μην επιτρέπει την είσοδο σε κανένα πακέτο και σύνδεση εκτός εάν ο τύπος της κίνησης και της σύνδεσης έχει ρητώς επιτραπεί. Αυτή η προσέγγιση θεωρείται περισσότερο ασφαλής από το να επιτρέπει αρχικά την είσοδο σε όλες τις συνδέσεις και πακέτα, εξαιρώντας κατόπιν συγκεκριμένους τύπους σύνδεσης και κίνησης.

(β) Η διαμόρφωση των firewalls γίνεται με βάση την αποτίμηση κινδύνων δικτύου και οφείλει να ανανεώνεται (αν χρειάζεται) κάθε φορά που τροποποιείται η Αναφορά Αποτίμησης Κινδύνων ή και σε προγραμματισμένα, τακτά χρονικά διαστήματα. Η πολιτική ασφάλειας περιμέτρου καθορίζει μια τυπική διαδικασία για τη διαχείριση των προσθέσεων και αφαιρέσεων των κανόνων του firewall.

(γ) Ο πάροχος διαδικτύου θα επιτρέπει την είσοδο από το Διαδίκτυο προς το εσωτερικό έμπιστο δίκτυο μέσω του firewall εκείνων μόνο των δικτυακών συνόδων που έχουν ισχυρή ταυτοποίηση και κρυπτογράφηση.

(δ) Το firewall πρέπει να ελέγχεται και παρακολουθείται συνεχώς για τον εντοπισμό παραβιάσεων ή κακής διαχείρισης, πιθανώς και με τη χρήση Συστημάτων Ανίχνευσης Επισυνδέσεων.

(ε) Το firewall πρέπει να ενημερώνει τον Υπεύθυνο Πολιτικής Ασφάλειας Περιμέτρου σε σχεδόν πραγματικό χρόνο σχετικά με κάθε στοιχείο που ενδέχεται να χρειάζεται άμεσης εξέτασης (όπως μια εισβολή στο σύστημα) και αντιμετώπισης.

(στ) Η δρομολόγηση με βάση τη διεύθυνση πηγής (source routing) πρέπει να είναι απενεργοποιημένη σε όλα τα συστήματα firewall και τους εξωτερικούς δρομολογητές.

(ζ) Το σύστημα firewall πρέπει να καταγράφει λεπτομερώς και να αποθηκεύει για ικανοποιητικό χρονικό διάστημα όλες τις δικτυακές συνόδους ώστε να μπορούν να εξεταστούν για ανωμαλίες offline. Στο αποθηκευμένο αυτό υλικό έχει πρόσβαση μόνο ο Υπεύθυνος Πολιτικής Ασφάλειας Περιμέτρου.

(η) Ο Υπεύθυνος Πολιτικής Ασφάλειας Περιμέτρου οφείλει να κρατά γραπτώς τεκμηρίωση της διαμόρφωσης και λειτουργίας του συστήματος firewall, συμπεριλαμβανόμενων πληροφοριών σχετικά με τη λειτουργία του δικτύου (διάγραμμα δικτύου, διευθύνσεις IP, και άλλα), καθώς και όλων των υπηρεσιών και των τύπων κίνησης που εξουσιοδοτούνται να διατρέξουν το firewall.

(θ) Ο Υπεύθυνος Πολιτικής Ασφάλειας Περιμέτρου οφείλει να αξιολογεί κάθε νέα έκδοση του λογισμικού του συστήματος firewall και να αποφασίζει εάν η ανανέωσή του είναι αναγκαία. Όλες οι προτεινόμενες από τον κατασκευαστή τροποποιήσεις (patches), που είναι σχετικές με την ασφάλεια του συστήματος firewall, πρέπει να υλοποιούνται άμεσα.

Άρθρο 5
Συστήματα Ανίχνευσης Επισυνδέσεων

1. Ο πάροχος διαδικτύου υποχρεούται να χρησιμοποιεί συστήματα ανίχνευσης επισυνδέσεων για την ενίσχυση της προστασίας του δικτύου του, σύμφωνα με την πολιτική ασφάλειας περιμέτρου που έχει ορίσει, χωρίς διακοπή (24 ώρες το 24ωρο). Διακοπή της λειτουργίας των συστημάτων αυτών επιτρέπεται μόνο για διαδικασίες συντήρησης ή αναβάθμισής τους, εκτός εάν συντρέχουν περιπτώσεις ανωτέρας βίας (π.χ. βλάβες) ή η διακοπή οφείλεται σε λόγους που δεν άγονται στο πεδίο δραστηριότητας και ευθύνης του παρόχου.

2. Η λειτουργικότητα των συστημάτων ανίχνευσης επισυνδέσεων πρέπει τουλάχιστον να περιλαμβάνει την παρακολούθηση των επισφαλών γεγονότων στο δίκτυο, καθώς και την παθητική (passive) αντίδρασή τους σε περίπτωση διαπίστωσης επισύνδεσης. Η παθητική αντίδραση περιλαμβάνει τουλάχιστον την ενεργοποίηση των συναγερμών που υποστηρίζει το σύστημα και την ειδοποίηση του Υπεύθυνου Πολιτικής Ασφάλειας Περιμέτρου. Συνιστάται όμως το σύστημα ανίχνευσης επισύνδεσης να ορίζει και να μπορεί να επιτελέσει επιπλέον ενεργές (active) αντιδράσεις σε περίπτωση διαπίστωσης επισύνδεσης. Ενδεικτικά και όχι περιοριστικά αναφέρονται τα εξής παραδείγματα ενεργής αντίδρασης: συλλογή επιπλέον πληροφοριών, μεταβολή του δικτυακού περιβάλλοντος, και απευθείας αντίδραση κατά των εισβολέων.

3. Η διαμόρφωση των συστημάτων ανίχνευσης επισυνδέσεων γίνεται με βάση την αποτίμηση κινδύνων δικτύου και οφείλει να ανανεώνεται (αν χρειάζεται) κάθε φορά που τροποποιείται η Αναφορά Αποτίμησης Κινδύνων ή και σε προγραμματισμένα, τακτά χρονικά διαστήματα. Η πολιτική ασφάλειας περιμέτρου καθορίζει μια τυπική διαδικασία για τη διαμόρφωση των συστημάτων ανίχνευσης επισυνδέσεων.

4. Τα συστήματα ανίχνευσης θα πρέπει να ελέγχονται σε τακτά χρονικά διαστήματα, από το προσωπικό που είναι υπεύθυνο για το χειρισμό και τη λειτουργία τους, ώστε το λογισμικό τους να είναι ενημερωμένο.

5. Τα διάφορα γεγονότα που ανιχνεύονται από το σύστημα ανίχνευσης επισυνδέσεων πρέπει να καταγράφονται και να αποθηκεύονται από το σύστημα για περαιτέρω επεξεργασία. Σημαντικά γεγονότα που καταγράφονται από το σύστημα, θα αναλύονται διεξοδικά από τον Υπεύθυνο Πολιτικής Ασφάλειας Περιμέτρου και θα καταγράφονται σε ειδική Φόρμα Καταγραφής Επισυνδέσεων που θα ορίζεται από την πολιτική ασφάλειας περιμέτρου. Περιοδικά, ή ύστερα από έλεγχο από την ΑΔΑΕ, ο πάροχος διαδικτύου είναι υποχρεωμένος να αποστέλλει τις φόρμες αυτές στην ΑΔΑΕ.

ΚΕΦΑΛΑΙΟ III
ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΗΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΟΥ ΕΞΟΠΛΙΣΜΟΥ

Άρθρο 6
Ανάγκη Ύπαρξης Πολιτικής Εγκατάστασης και Διαχείρισης Τηλεπικοινωνιακού Εξοπλισμού

1. Κάθε πάροχος διαδικτύου υποχρεούται να διαθέτει Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού ως μέρος της Πολιτικής Ασφάλειάς του.

2. Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού εξασφαλίζει ότι τυχόν αλλαγές στον υπάρχοντα εξοπλισμό (υλικό, λογισμικό και διαμόρφωση αυτών) καθώς και η εισαγωγή καινούργιου εξοπλισμού στη λειτουργία του παρόχου διαδικτύου γίνεται κατά τέτοιο τρόπο ώστε να διασφαλίζεται το απόρρητο των επικοινωνιών και να μην παραβιάζεται η Πολιτική Ασφάλειας του παρόχου διαδικτύου.

3. Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού μπορεί να είναι κοινή για όλες τις οργανικές μονάδες του παρόχου διαδικτύου ή να διαφοροποιείται ανάλογα με τις ειδικές ανάγκες κάθε οργανικής μονάδας. Σε κάθε περίπτωση όμως θα πρέπει να τηρούνται οι βασικές αρχές εγκατάστασης και διαχείρισης που περιγράφονται στον παρόντα Κανονισμό.

Άρθρο 7
Σκοπός και Περιεχόμενο της Πολιτικής Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού

1. Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού, στο πλαίσιο της απαίτησης για διασφάλιση του απορρήτου των επικοινωνιών και της τήρησης της Πολιτικής Ασφαλείας του παρόχου διαδικτύου αλλά και γενικότερα στο πλαίσιο της εύρυθμης λειτουργίας του παρόχου διαδικτύου, καθορίζει ένα συστηματικό τρόπο για:

(α) Τη δημιουργία πλήρους ιστορικού αναφορικά με τις αλλαγές που έχουν πραγματοποιηθεί στον τηλεπικοινωνιακό εξοπλισμό του παρόχου διαδικτύου.

(β) Την εκτίμηση του χρόνου διακοπής της παροχής διαφόρων υπηρεσιών που σχετίζονται με πραγματοποιούμενες αλλαγές.

(γ) Τον συντονισμό των αλλαγών που πραγματοποιούνται στον τηλεπικοινωνιακό εξοπλισμό έτσι ώστε αλλαγές σε κάποιο στοιχείο του εξοπλισμού να μην επηρεάζουν / επιφέρουν αλλαγές σε άλλα στοιχεία του εξοπλισμού.

(δ) Την ελαχιστοποίηση της πιθανότητας για εκδήλωση επισυνδέσεων και άλλων παρόμοιων απειλών εναντίον του τηλεπικοινωνιακού εξοπλισμού του παρόχου διαδικτύου.

2. Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού σε έναν πάροχο διαδικτύου περιλαμβάνει κατ' ελάχιστο:

(α) Διαδικασίες για τη δοκιμή και την εγκατάσταση νέου τηλεπικοινωνιακού εξοπλισμού.

(β) Διαδικασίες για την καταγραφή των αλλαγών που πραγματοποιούνται σε υπάρχοντα τηλεπικοινωνιακό εξοπλισμό.

(γ) Διαδικασίες για την ενημέρωση του παρόχου διαδικτύου αναφορικά με την πραγματοποίηση αλλαγών σε υπάρχοντα τηλεπικοινωνιακό εξοπλισμό.

(δ) Διαδικασίες για το καθορισμό αρμοδιοτήτων αναφορικά με την διαχείριση και τη διαμόρφωση τηλεπικοινωνιακού εξοπλισμού.

(ε) Διαδικασίες για την εξουσιοδότηση μελών του προσωπικού του παρόχου διαδικτύου, τα οποία θα εφαρμόζουν την εν λόγω πολιτική συνολικά για όλες τις οργανικές μονάδες του παρόχου διαδικτύου ή/και ανά οργανική μονάδα ξεχωριστά.

Άρθρο 8
Εγκατάσταση Τηλεπικοινωνιακού Εξοπλισμού

1. Ο τηλεπικοινωνιακός εξοπλισμός ενός παρόχου διαδικτύου εγκαθίσταται εντός των ορίων της περιμέτρου του παρόχου διαδικτύου και σύμφωνα με τα όσα ορίζονται στην αντίστοιχη Πολιτική Ασφαλείας Περιμέτρου. Εξαιρούνται περιπτώσεις για τις οποίες τεκμηριώνεται απαίτηση για εγκατάσταση εκτός της περιμέτρου προκειμένου να επιτευχθεί ορθή λειτουργία του εξοπλισμού ή/και των υπηρεσιών που βασίζονται στη λειτουργία του.

2. Η εγκατάσταση του εξοπλισμού γίνεται σε δύο τουλάχιστον στάδια και περιλαμβάνει κατ' ελάχιστο τα ακόλουθα βήματα:

Στάδιο Προετοιμασίας:

(α) Ελέγχονται η πληρότητα και η έκταση της προσφερόμενης τεκμηρίωσης αναφορικά με την εγκατάσταση, τη διαμόρφωση, τη χρήση και τη συντήρηση του εξοπλισμού δίνοντας έμφαση σε ότι αφορά στα χαρακτηριστικά ασφάλειάς του και τις δυνατότητες προστασίας και άρσης του απορρήτου. Η τεκμηρίωση θα πρέπει να περιλαμβάνει ένα καλά καθορισμένο σύνολο από δοκιμές αποδοχής του εξοπλισμού. Εφόσον ο υπό εγκατάσταση εξοπλισμός περιλαμβάνει λογισμικό το οποίο έχει αναπτυχθεί εσωτερικά τότε η τεκμηρίωση θα πρέπει να περιλαμβάνει ανάλυση / σχολιασμό σε επίπεδο πηγαίου κώδικα.

(β) Εφόσον η εγκατάσταση εξοπλισμού περιλαμβάνει και εγκατάσταση λογισμικού τότε ελέγχεται η συμμόρφωση του λογισμικού με καθιερωμένα διεθνή πρότυπα ή διεθνώς διαδεδομένες πρακτικές.

(γ) Αποτιμάται ο κίνδυνος, αναφορικά με την ορθή λειτουργία του παρόχου διαδικτύου, που μπορεί να προκύψει από ενδεχόμενη δυσλειτουργία του υπό εγκατάσταση τηλεπικοινωνιακού εξοπλισμού. Η αποτίμηση του κινδύνου περιλαμβάνει και την καταγραφή των αλληλεξαρτήσεων του υπό εγκατάσταση τηλεπικοινωνιακού εξοπλισμού με τα υπάρχοντα τμήματα του τηλεπικοινωνιακού εξοπλισμού που βρίσκονται σε λειτουργία στον πάροχο διαδικτύου. Επίσης η διαδικασία αποτίμησης του κινδύνου καθορίζει κατά πόσον οι δοκιμές αποδοχής του εξοπλισμού θα πρέπει να διεξαχθούν σε ξεχωριστό περιβάλλον δοκιμών ή όχι. Η αποτίμηση του κινδύνου γίνεται τόσο σε επίπεδο υλικού και λογισμικού όσο και σε επίπεδο δικτυακής επικοινωνίας.

(δ) Στην περίπτωση αναβάθμισης λογισμικού αποτιμάται η εξάρτηση του εν λόγω λογισμικού από το λειτουργικό σύστημα που είναι εν χρήσει στο αντίστοιχο υλικό καθώς και από βιβλιοθήκες λογισμικού οι οποίες είναι τυχόν εν χρήσει στο αντίστοιχο υλικό.

(ε) Καθορίζεται ποια χαρακτηριστικά του εξοπλισμού, που σχετίζονται με την ασφάλεια και τη διασφάλιση του απορρήτου, πρέπει να ενεργοποιηθούν και με ποιο τρόπο.

Στάδιο Εγκατάστασης και Ελέγχου Ορθής Λειτουργίας:

(στ) Ο εξοπλισμός εγκαθίσταται είτε στο ξεχωριστό περιβάλλον δοκιμής είτε στο περιβάλλον παραγωγής του παρόχου διαδικτύου σύμφωνα με τη διαδικασία αποτίμησης κινδύνου. Ελέγχονται οι λειτουργίες του εξοπλισμού και διαπιστώνονται τυχόν προβλήματα. Τα προβλήματα συζητούνται με τον προμηθευτή του εξοπλισμού και γίνεται προσπάθεια επίλυσής τους.

(ζ) Εφόσον οι δοκιμές του υπό εγκατάσταση εξοπλισμού γίνονται σε συνεργασία με τηλεπικοινωνιακό εξοπλισμό ο οποίος ευρίσκεται σε περιβάλλον παραγωγής τότε είναι επιθυμητό οι δοκιμές αυτές να λαμβάνουν χώρα σε περιόδους χαμηλής τηλεπικοινωνιακής κίνησης (περιόδους μη αιχμής). Για την πραγματοποίηση των δοκιμών θα πρέπει να χρησιμοποιούνται όπου αυτό είναι δυνατό, δοκιμαστικά δεδομένα.

3. Οι ενέργειες που περιγράφονται στις παραγράφους 1 και 2 του παρόντος Άρθρου πραγματοποιούνται από εξουσιοδοτημένο προσωπικό του παρόχου διαδικτύου, σύμφωνα με τις αρμοδιότητες που έχουν καθορισθεί από την Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού. Σε περίπτωση σύμβασης υπεργολαβίας, η τελική ευθύνη της τήρησης της Πολιτικής Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού παραμένει στον πάροχο διαδικτύου.

4. Το εξουσιοδοτημένο προσωπικό του παρόχου διαδικτύου με αιτιολογημένη έκθεσή του προτείνει την αποδοχή ή απόρριψη του εξοπλισμού στις ενδιαφερόμενες μονάδες του παρόχου διαδικτύου. Ο Υπεύθυνος Ασφάλειας του παρόχου διαδικτύου λαμβάνει γνώση της εκθέσεως. Στην περίπτωση που στην έκθεση προτείνεται η αποδοχή του εξοπλισμού τότε αυτός τίθεται σε λειτουργία στο περιβάλλον παραγωγής.

Άρθρο 9
Διαχείριση Τηλεπικοινωνιακού Εξοπλισμού

1. Η πρόσβαση στον εγκατεστημένο εξοπλισμό καθορίζεται από την ισχύουσα Πολιτική Ασφάλειας Περιμέτρου.

2. Το εξουσιοδοτημένο προσωπικό του παρόχου διαδικτύου θα πρέπει να ενημερώνεται αναφορικά με κάθε πρόβλημα ασφάλειας ή/και αναθεώρησης υλικού και λογισμικού που σχετίζεται με την ασφάλεια του τηλεπικοινωνιακού εξοπλισμού το οποίο διαπιστώνεται από κατασκευαστή ή από έγκυρους οργανισμούς σχετιζόμενους με την ασφάλεια, να αξιολογεί άμεσα κάθε σχετική πληροφορία αυτής της μορφής και, εφόσον διαπιστώνει ότι αφορά στον εξοπλισμό του παρόχου, να προβαίνει στις κατάλληλες αναβαθμίσεις.

3. Κατά τη διαδικασία διευθυνσιοδότησης του τηλεπικοινωνιακού εξοπλισμού δεν θα πρέπει να ενθαρρύνεται η χρήση δημοσίως γνωστών δικτυακών αναγνωριστικών (ενδεικτικά αναφέρονται διευθύνσεις IP, hostnames κ.λ.π.) εκτός από τις περιπτώσεις στις οποίες τεκμηριώνεται σχετική απαίτηση προκειμένου να επιτευχθεί ορθή λειτουργία του εξοπλισμού ή/και των υπηρεσιών που βασίζονται στη λειτουργία του.

4. Κάθε διακομιστής που αποτελεί μέρος τηλεπικοινωνιακού εξοπλισμού παρόχου θα πρέπει, κατά προτίμηση:

(α) Να χρησιμοποιείται για την παροχή μίας μόνο υπηρεσίας, ώστε να ελαχιστοποιείται η πιθανότητα διαχειριστικών λαθών και να μειώνονται τα περιθώρια για παραβίαση της ασφάλειας του διακομιστή με εκδήλωση επισυνδέσεων και άλλων αντίστοιχων απειλών. Η χρήση εξοπλισμού για περισσότερες από μία υπηρεσίες επιτρέπεται μόνο εφόσον ο κίνδυνος που προκύπτει από τέτοια κοινή χρήση έχει εξεταστεί από την διαδικασία αποτίμησης κινδύνου. Στην περίπτωση που ο διακομιστής χρησιμοποιείται για την παροχή περισσότερων της μιας υπηρεσιών, θα πρέπει να καταβάλλεται κάθε δυνατή προσπάθεια για απενεργοποίηση υπηρεσιών που δεν χρησιμοποιούνται, ιδιαίτερα εφόσον οι εν λόγω υπηρεσίες σχετίζονται με τη διαδικτυακή πρόσβαση.

(β) Να μη χρησιμοποιείται ως σταθμός εργασίας.

5. Σε κάθε δρομολογητή που αποτελεί μέρος τηλεπικοινωνιακού εξοπλισμού θα πρέπει, όποτε είναι εφικτό, να λαμβάνει χώρα:

(α) Απενεργοποίηση υπηρεσιών που δεν χρησιμοποιούνται.

(β) Αποτίμηση των δικτυακών διευθύνσεων, θυρών και πρωτοκόλλων με βάση τα οποία δρομολογούνται δεδομένα από το δρομολογητή.

(γ) Απενεργοποίηση της υπηρεσίας δρομολόγησης για δικτυακές διευθύνεις, θύρες και πρωτόκολλα που δεν περιλαμβάνονται στην ως άνω αποτίμηση.

6. Τυχόν διαχείριση τηλεπικοινωνιακού εξοπλισμού από απόσταση θα πρέπει να γίνεται μέσα από ασφαλείς διαύλους επικοινωνίας (ενδεικτικά αναφέρονται μισθωμένη γραμμή με κρυπτογράφηση, σύνδεση VPN κλπ.).

7. Ο χειρισμός των κωδικών ασφαλείας του τηλεπικοινωνιακού εξοπλισμού υπάγεται στην Πολιτική Κωδικών Ασφάλειας σύμφωνα με τον Κανονισμό για τη Διασφάλιση του Απορρήτου Εφαρμογών Διαδικτύου και Χρήστη.

8. Η διαμόρφωση του τηλεπικοινωνιακού εξοπλισμού θα πρέπει να ενεργοποιεί τις αντίστοιχες δυνατότητες καταγραφής ώστε να καθίσταται εφικτή η άρση του απορρήτου σύμφωνα με την κείμενη νομοθεσία.

9. Σε περίπτωση που ο τηλεπικοινωνιακός εξοπλισμός παρέχει τη δυνατότητα υλοποίησης πολλαπλών επιπέδων δικαιωμάτων πρόσβασης σε πόρους και δεδομένα του, πέραν της χρήσης κωδικών ασφαλείας, η διαμόρφωση του εξοπλισμού θα πρέπει να αξιοποιεί αυτή τη δυνατότητα. Με τον τρόπο αυτό μειώνεται η πιθανότητα παραβίασης της ασφαλείας και του απορρήτου είτε από τυχαία ενέργεια μη εξουσιοδοτημένου χρήστη ή από προσχεδιασμένη απειλή.

10. Στον εξοπλισμό επιτρέπεται η εγκατάσταση λογισμικού μόνο από το εξουσιοδοτημένο προσωπικό και μόνο για τους σκοπούς υποστήριξης του εξοπλισμού και των υπηρεσιών που προσφέρει.

11. Στα πλαίσια της Πολιτικής Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού το ειδικά εξουσιοδοτημένο προσωπικό του παρόχου διαδικτύου καταγράφει σε μόνιμη βάση όλες τις πράξεις που σχετίζονται με εγκατάσταση, απεγκατάσταση, αναβάθμιση, αλλαγή διαμόρφωσης του τηλεπικοινωνιακού εξοπλισμού του παρόχου διαδικτύου. Η καταγραφή γίνεται εντύπως σε ειδικό βιβλίο ή/και ηλεκτρονικά σε βάση δεδομένων του παρόχου διαδικτύου.

12. Με την ως άνω καταγραφή θα εξασφαλίζεται επίσης ότι στον τηλεπικοινωνιακό εξοπλισμό του παρόχου διαδικτύου δεν έχει εγκατασταθεί παράνομο ή επικίνδυνο λογισμικό.

13. Πρόσβαση στην ως άνω καταγραφή έχει μόνο το εξουσιοδοτημένο προσωπικό του παρόχου.

14. Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού θα πρέπει να προβλέπει τη διατήρηση των παλαιών εκδόσεων του λογισμικού για ορισμένο χρονικό διάστημα με σκοπό την επαναφορά τους στα συστήματα του παρόχου διαδικτύου στην περίπτωση που διαπιστωθεί πρόβλημα λειτουργίας το οποίο οφείλεται σε εγκατάσταση νέας έκδοσης λογισμικού ή σε αναβάθμιση λογισμικού. Οι ακριβείς διαδικασίες διατήρησης και επαναφοράς των παλαιών εκδόσεων του λογισμικού ορίζονται κατά περίπτωση από τον κάθε πάροχο διαδικτύου.

15. Τα τμήματα του τηλεπικοινωνιακού εξοπλισμού του παρόχου διαδικτύου, τα οποία είναι δυνατό να τρωθούν από ιούς, θα πρέπει να προστατεύονται από κατάλληλο λογισμικό κατά των ιών.

16. Η Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού προβλέπει συγκεκριμένες ενέργειες αναφορικά με την ασφάλεια και το απόρρητο κατά τη διαδικασία απεγκατάστασης τηλεπικοινωνιακού εξοπλισμού του παρόχου διαδικτύου. Με τις ενέργειες αυτές θα πρέπει να διασφαλίζεται ότι η πληροφορία που έχει εγγραφεί μόνιμα στον εν λόγω εξοπλισμό (π.χ. σε μνήμες ROM, σκληρούς δίσκους, μαγνητικές ταινίες κλπ.) διαγράφεται οριστικά και δεν μπορεί να χρησιμοποιηθεί από τρίτους προκειμένου να παραβιασθεί η ασφάλεια του παρόχου διαδικτύου.

ΚΕΦΑΛΑΙΟ IV
ΠΟΛΙΤΙΚΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ

Άρθρο 10
Γενικά

1. Η Πολιτική Αντιγράφων Ασφάλειας περιλαμβάνει τις διαδικασίες και τους ελέγχους που θα εξασφαλίσουν ότι ο τηλεπικοινωνιακός εξοπλισμός μπορεί να ανακτήσει τη λειτουργία εντός μιας λογικής χρονικής περιόδου μετά από οποιαδήποτε ζημιά που μπορεί να οφείλεται σε κακόβουλες επιθέσεις στο δικτυακό εξοπλισμό.

2. Ο σκοπός της πολιτικής αυτής είναι να καθορίζει τους κανόνες και τις διαδικασίες αντιγράφων ασφάλειας και ανάκτησης δεδομένων για να αποτραπεί η απώλεια στοιχείων στην περίπτωση διακοπής της λειτουργίας του συστήματος του παρόχου διαδικτύου.

Άρθρο 11
Περιεχόμενο

1. Τα Αντίγραφα Ασφάλειας στην παρούσα πολιτική αναφέρονται στα δεδομένα διάρθρωσης των δικτυακών στοιχείων.

2. Κάθε πάροχος διαδικτύου πρέπει να αναπτύξει και να συντηρήσει ένα σχέδιο για να μπορεί να ανταποκρίνεται σε περιπτώσεις εκτάκτου ανάγκης του συστήματος μετά από κακόβουλες επιθέσεις περιλαμβάνοντας την εκτέλεση αντιγράφων ασφαλείας, την παροχή διαδικασιών που μπορούν να χρησιμοποιηθούν για να διευκολύνουν τη συνέχιση της λειτουργίας σε περίπτωση ανάγκης και την ανάκτηση από μια επίθεση. Πιο συγκεκριμένα:

(α) Πρέπει να αναπτυχθεί και να τεκμηριωθεί μια διαδικασία ανάλυσης της ευαισθησίας, των ευπαθειών, και της ασφάλειας των προγραμμάτων και των πληροφοριών που λαμβάνουν, χειρίζονται, αποθηκεύουν, ή/και μεταδίδουν τα δικτυακά στοιχεία ώστε να προσδιοριστούν τα στοιχεία για τα οποία θα πρέπει να αποθηκεύονται.

(β) Η συχνότητα και η έκταση των αντιγράφων ασφαλείας πρέπει να είναι σύμφωνα με τη σημασία των πληροφοριών και του αποδεκτού κινδύνου όπως καθορίζεται μετά από την αντίστοιχη ανάλυση.

(γ) Ένα σχέδιο ανάκτησης δεδομένων πρέπει να τεκμηριωθεί και να ενημερώνεται σε τακτά χρονικά διαστήματα για να δημιουργήσει και να διατηρήσει, για μια συγκεκριμένη χρονική περίοδο, ανακτήσιμα ακριβή αντίγραφα των πληροφοριών.

(δ) Ένα σχέδιο αποκατάστασης πρέπει να αναπτυχθεί και να τεκμηριωθεί, έτσι ώστε να επιτρέπει στον πάροχο διαδικτύου να αποκαταστήσει οποιαδήποτε απώλεια στοιχείων σε περίπτωση αποτυχίας του συστήματος και των δικτυακών πόρων μετά από κακόβουλη επίθεση.

(ε) Ένα σχέδιο λειτουργίας τρόπου έκτακτης ανάγκης πρέπει να αναπτυχθεί και να τεκμηριωθεί, το οποίο να επιτρέπει στον πάροχο διαδικτύου να συνεχίσει να λειτουργεί σε περίπτωση αποτυχίας του συστήματος.

(στ) Διαδικασίες δοκιμών και αναθεώρησης πρέπει να αναπτυχθούν και να τεκμηριωθούν, οι οποίες να απαιτούν την περιοδική δοκιμή των σχεδίων έκτακτης ανάγκης (contingency plans) για να ανακαλύψουν τυχόν αδυναμίες.

(ζ) Στα αντίγραφα ασφαλείας πρέπει να διατίθεται το ίδιο επίπεδο προστασίας με τα αρχικά στοιχεία.

(η) Τα εφεδρικά αντίγραφα ασφαλείας και οι διαδικασίες αντιγραφής θα πρέπει να εξετάζονται περιοδικά για να εξασφαλισθεί ότι είναι δυνατό να ανακτηθούν.

Άρθρο 12
Ασφάλεια Αντιγράφων Δικτυακών Στοιχείων

1. Σε περίπτωση βλάβης κάποιας δικτυακής διάταξης, όπως δρομολογητές, μεταγωγείς (switch), κόμβοι (hub) και firewalls ή ακόμα και σε περίπτωση κακόβουλης αλλαγής της διάρθρωσης των διατάξεων αυτών, είναι απαραίτητος ο επαναπρογραμματισμός των στοιχείων αυτών στην αρχική τους κατάσταση. Για αυτό το λόγο θα πρέπει διάφορα αρχεία που προσδιορίζουν την κατάσταση και τη διάρθρωση των συσκευών αυτών να αντιγράφονται, και συγκεκριμένα:

(α) Τα δεδομένα διάρθρωσης μιας δικτυακής διάταξης (λογισμικό συστήματος, αρχεία σύνθεσης του λογισμικού, αρχεία βάσεων δεδομένων, κλπ.) πρέπει να αντιγράφονται ημερησίως, εβδομαδιαίως και μηνιαίως, έτσι ώστε σε περίπτωση αποτυχίας του συστήματος, τα δεδομένα και τα αρχεία σύνθεσης του λογισμικού (configuration files) να μπορούν να ανακτηθούν.

(β) Τα εφεδρικά αντίγραφα πρέπει να αποθηκεύονται με ασφαλή τρόπο σε αρχεία μόνο αναγνώσιμα έτσι ώστε τα αποθηκευμένα δεδομένα να μην επεγγράφονται (overwrite) ακούσια και πρέπει να κλειδώνονται ώστε τα δεδομένα να είναι προσβάσιμα μόνο σε εξουσιοδοτημένο προσωπικό.

(γ) Μια λύση θα ήταν η ύπαρξη ενός εφεδρικού firewall, που θα έχει την ίδια σύνθεση με το firewall που χρησιμοποιείται. Το firewall αυτό θα μπορούσε να τεθεί σε λειτουργία σε περίπτωση βλάβης του αρχικού και να χρησιμοποιείται ενώ το άλλο είναι υπό επισκευή. Τουλάχιστον ένα firewall πρέπει να έχει διαρθρωθεί και να διαφυλάσσεται, ώστε σε περίπτωση αποτυχίας, αυτό το εφεδρικό firewall να μπορεί να χρησιμοποιηθεί για την προστασία του δικτύου.

2. Σημαντικό για τον πάροχο διαδικτύου είναι επίσης η παροχή προστασίας στους διακομιστές του δίκτυου του και η ανάκτηση αρχείων στην περίπτωση απώλειας αυτών. Οι διαχειριστές δικτύων μπορεί να παρέχουν διάφορες μεθόδους παροχής εφεδρικών αντιγράφων, όπως πλήρη, αυξητική και διαφορική αντιγραφή αρχείων. Μια διαφορετική μέθοδος αντιγραφής είναι η Δικτυακή Αντιγραφή αρχείων, στην οποία κρυπτογραφημένα δεδομένα με αυτόματο και ασφαλή τρόπο αντιγράφονται και αποθηκεύονται σε μια περιοχή εκτός του εσωτερικού δικτύου του παρόχου διαδικτύου.

ΚΕΦΑΛΑΙΟ V
ΔΙΑΔΙΚΑΣΙΑ ΧΕΙΡΙΣΜΟΥ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Άρθρο 13
Γενικά

1. Κάθε πάροχος διαδικτύου οφείλει να διαθέτει σαφή Διαδικασία Χειρισμού Περιστατικών Ασφάλειας (Δ.Χ.Π.Α) τα οποία απειλούν την ασφάλεια των επικοινωνιακών υποδομών αλλά και τη διασφάλιση του απορρήτου των επικοινωνιών που διεξάγονται μέσω του παρόχου.

2. Σε κάθε περίπτωση όπου:

(α) διαπιστώνεται κίνδυνος για την διασφάλιση του απορρήτου,

(β) έχει καταγγελθεί παραβίαση απορρήτου,

(γ) υπάρχουν σοβαρές υπόνοιες ότι δε διασφαλίζεται το απόρρητο των επικοινωνιών,

ο πάροχος διαδικτύου οφείλει να ενεργοποιεί άμεσα την Δ.Χ.Π.Α.

3. Στόχοι της διαδικασίας είναι να:

(α) Καταγραφούν όλες οι λεπτομέρειες του περιστατικού.

(β) Να ενημερωθούν οι αρμόδιοι (του παρόχου διαδικτύου αλλά και φορείς όπως η ΑΔΑΕ) και οι χρήστες.

(γ) Να διασφαλιστεί το δυνατόν συντομότερο το απόρρητο.

(δ) Να διερευνηθούν τα αίτια και να βρεθούν τα πιθανά σφάλματα του παρόχου διαδικτύου ή και άλλων προσώπων.

Άρθρο 14
Περιεχόμενο

1. Η Δ.Χ.Π.Α. πρέπει να περιέχει τουλάχιστον τα σημεία που περιγράφονται στο παρόν άρθρο.

2. Πρέπει να ορίζεται ομάδα άμεσου χειρισμού του συμβάντος αποτελούμενη από εξειδικευμένους τεχνικούς αλλά και διοικητικά στελέχη. Τα τεχνικά στελέχη έχουν την ευθύνη να επιβεβαιώσουν το συμβάν και να προβούν άμεσα στην αποκατάσταση του προβλήματος. Τα διοικητικά στελέχη φέρουν την ευθύνη αξιολόγησης και διαχείρισης του συμβάντος σε συνεργασία με την τεχνική ομάδα.

3. Κάθε συμβάν θα πρέπει να αναφέρεται ώστε να είναι δυνατή η άμεση αντιμετώπισή του. Για αυτό το λόγο θα πρέπει να οριστεί ένα ή περισσότερα άτομα στα οποία θα πρέπει να αναφέρεται άμεσα η εκδήλωση ενός περιστατικού ασφάλειας, από οποιοδήποτε μέλος του προσωπικού του παρόχου, όταν αυτό γίνεται αντιληπτό. Το άτομο ή τα άτομα αυτά θα πρέπει να γνωστοποιούνται σε όλο το προσωπικό, μαζί με πιθανούς τρόπους επικοινωνίας (τηλέφωνα, fax, email ή ό,τι άλλο κρίνεται αναγκαίο).

4. Κάθε συμβάν πρέπει να αξιολογείται και με βάση την αξιολόγησή του, κρίνεται ο τρόπος με τον οποίο πρέπει να αντιμετωπιστεί. Ανάλογα με την κρισιμότητα του περιστατικού ενεργοποιείται και η κατάλληλη διάταξη της Δ.Χ.Π.Α.

5. Επίσης πρέπει να ορίζεται η επικοινωνιακή πολιτική για κάθε περίπτωση ανάλογου περιστατικού. Αναλόγως με την κρισιμότητα του συμβάντος ειδοποιούνται τα κατάλληλα στελέχη του παρόχου διαδικτύου. Σε περίπτωση κρίσιμου περιστατικού πρέπει να ειδοποιούνται σταδιακά υψηλόβαθμα στελέχη του παρόχου διαδικτύου, τα οποία φέρουν και την ευθύνη καταγγελίας του περιστατικού στους αρμόδιους φορείς και την ΑΔΑΕ.

6. Ο παρακάτω πίνακας είναι ενδεικτικός για τον τρόπο με τον οποίο αντιμετωπίζονται αντίστοιχα συμβάντα με βάση την κρισιμότητά τους.

Κρισιμότητα	Ομάδα άμεσης επέμβασης Περιλαμβάνει στοιχεία επικοινωνίας, και ρόλο του κάθε προσώπου	Ενέργειες Περιλαμβάνουν τόσο τεχνικές επιταγές και σχέδιο αποκατάστασης του απορρήτου, όσο και διοικητικές ενέργειες.	Επικοινωνιακή πολιτική Περιλαμβάνει λίστα των φορέων και ατόμων οι οποίοι πρέπει να λάβουν γνώση του συμβάντος, καθώς και τη συχνότητα ενημέρωσης του κάθε φορέα ή προσώπου.
Κρίσιμη	• Τεχνική • Διοικητική	• Τεχνική • Διοικητική	• Πάροχος Διαδικτύου • Φορείς
Σοβαρή	• Τεχνική • Διοικητική	• Τεχνική • Διοικητική	• Πάροχος Διαδικτύου • Φορείς
Πιθανή	• Τεχνική • Διοικητική	• Τεχνική • Διοικητική	• Πάροχος Διαδικτύου • Φορείς
Ελάχιστη	• Τεχνική • Διοικητική	• Τεχνική • Διοικητική	• Πάροχος Διαδικτύου • Φορείς

7. Ο πάροχος διαδικτύου οφείλει να διατηρεί την Δ.Χ.Π.Α. ενημερωμένη με σωστά στοιχεία επικοινωνίας για όλους του εμπλεκόμενους. Τα στοιχεία των προσώπων και φορέων που πρέπει να ειδοποιηθούν άμεσα στην περίπτωση που διαπιστώνεται κάποιο συμβάν πρέπει να επαρκούν για την άμεση ειδοποίησή τους.

8. Ακόμα, πρέπει να υπογραμμιστεί η αναγκαιότητα καταγραφής όλων των ενεργειών που εκτελέστηκαν από την τεχνική ομάδα, όλων των τεχνικών ευρημάτων, καθώς και όλων των επικοινωνιών κατά τη διάρκεια καταστολής του περιστατικού. Η καταγραφή των στοιχείων πρέπει να γίνεται με τρόπο σαφή και σε ειδικά έντυπα τα οποία περιγράφονται στην Δ.Χ.Π.Α. του παρόχου διαδικτύου.

9. Επίσης ο πάροχος διαδικτύου πρέπει να ελέγχει σε τακτά χρονικά διαστήματα την ετοιμότητα ενεργοποίησης όλων τον μηχανισμών και προσώπων που περιγράφονται στην Δ.Χ.Π.Α.

ΚΕΦΑΛΑΙΟ VI
ΔΙΑΔΙΚΑΣΙΑ ΕΛΕΓΧΟΥ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ

Άρθρο 15
Γενικά

1. Η διαδικασία ελέγχου ασφάλειας δικτύου πραγματοποιείται από την ομάδα ελέγχου ασφάλειας δικτύου του παρόχου διαδικτύου. Η ομάδα ελέγχου ασφάλειας δικτύου θα χρησιμοποιήσει συγκεκριμένο λογισμικό ελέγχου

για τη διεξαγωγή ηλεκτρονικής ανίχνευσης των δικτύων ή/και των συστημάτων προστασίας επιθέσεων ή οποιουδήποτε άλλου πληροφοριακού και δικτυακού συστήματος στον πάροχο διαδικτύου.

2. Ο έλεγχος ασφάλειας δικτύου πραγματοποιείται με σκοπό :

(α) Την εξακρίβωση ότι διασφαλίζεται η ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα πληροφοριών και πόρων.

(β) Την εξακρίβωση ότι διασφαλίζεται η συμφωνία των πιθανών περιστατικών που σχετίζονται με την ασφάλεια με την πολιτική ασφάλειας του παρόχου διαδικτύου.

(γ) Την παρακολούθηση ενεργειών των χρηστών, των χρηστών παρόχου και του συστήματος όπου αυτό κρίνεται αναγκαίο, ύστερα από σχετική ενημέρωση του χρήστη ή χρήστη παρόχου.

3. Η ομάδα ελέγχου ασφάλειας δικτύου επιτελεί τη διαδικασία ελέγχου ασφάλειας με τέτοιο τρόπο ώστε να μην εμποδίζεται η παροχή των υπηρεσιών του παρόχου διαδικτύου προς τους χρήστες ή χρήστες παρόχου.

4. Η ομάδα ελέγχου ασφάλειας δικτύου μπορεί να είναι εσωτερική, δηλαδή να απαρτίζεται από εργαζόμενους στον πάροχο διαδικτύου, ή εξωτερική, δηλαδή να απαρτίζεται από εξειδικευμένο προσωπικό άλλου φορέα, με τον οποίο συνάπτεται η κατάλληλη συμφωνία.

Άρθρο 16
Υποχρεώσεις Παρόχου

1. Κατά τη διαδικασία ελέγχου ασφάλειας δικτύου, ο πάροχος διαδικτύου επιτρέπει στην ομάδα ελέγχου ασφάλειας δικτύου την πρόσβαση στο δίκτυο και τα συστήματα προστασίας επιθέσεων, έως το επίπεδο το οποίο κρίνεται αναγκαίο ώστε να γίνει δυνατή η εκτέλεση των καθορισμένων ελέγχων.

2. Ο πάροχος διαδικτύου παρέχει τα αναγκαία πρωτόκολλα, τις δικτυακές συνδέσεις και τις πληροφορίες διευθυνσιοδότησης που είναι αναγκαία στην ομάδα ελέγχου ασφάλειας δικτύου για την εκτέλεση του λογισμικού ελέγχου και διάγνωσης του δικτύου. Η πρόσβαση αυτή μπορεί να συμπεριλαμβάνει:

(α) Πρόσβαση επιπέδου χρήστη ή/και συστήματος σε οποιαδήποτε διάταξη υπολογιστή και επικοινωνίας.

(β) Πρόσβαση σε πληροφορία (ηλεκτρονικής ή έντυπης μορφής) η οποία μπορεί να παραχθεί, μεταδοθεί ή αποθηκευτεί σε εξοπλισμό ή σε εγκαταστάσεις οι οποίες ανήκουν στον πάροχο διαδικτύου. Σε περίπτωση που η πληροφορία αυτή αφορά κάποιον χρήστη ή χρήστη παρόχου, ο πάροχος οφείλει να ενημερώνει το χρήστη ή χρήστη παρόχου για τη διαδικασία αυτή.

(γ) Πρόσβαση σε χώρους εργασίας (εργαστήρια, γραφεία, αποθηκευτικούς χώρους, κ.λ.π.)

(δ) Πρόσβαση με σκοπό την ενεργή παρακολούθηση και καταγραφή κίνησης πάνω από τα δίκτυα του παρόχου διαδικτύου.

Άρθρο 17
Έλεγχος Δικτύου

1. Η ομάδα ελέγχου ασφάλειας δικτύου πραγματοποιεί τον έλεγχο μόνο κατά τη διάρκεια των επιτρεπόμενων ημερομηνιών και ωραρίων που έχουν προσυμφωνηθεί με τον πάροχο διαδικτύου.

2. Σε περίπτωση που ο πάροχος διαδικτύου δε διαθέτει τον πλήρη έλεγχο πάνω στα δίκτυά του, ή η πρόσβαση στις υπηρεσίες διαδικτύου παρέχεται μέσω άλλων παρόχων διαδικτύου, οι τελευταίοι θα πρέπει να παράσχουν έγγραφη αποδοχή της διαδικασίας ελέγχου ασφάλειας δικτύου, κατά τη διάρκεια των προκαθορισμένων ημερομηνιών και ωραρίων.

3. Οι επιδόσεις ή/και η διαθεσιμότητα του δικτύου ενδέχεται να επηρεαστούν κατά τη διάρκεια των δοκιμών και των ελέγχων που θα πραγματοποιηθούν. Η ομάδα ελέγχου ασφάλειας δικτύου οφείλει να λαμβάνει όλα τα δυνατά μέτρα ώστε να ελαχιστοποιούνται όσο είναι δυνατό τέτοιες επιδράσεις. Όμως, η ομάδα ελέγχου ασφάλειας δικτύου απαλλάσσεται από οποιαδήποτε ευθύνη σχετικά με ζημιές οι οποίες ενδέχεται να προκύψουν ως αποτέλεσμα της μη διαθεσιμότητας του δικτύου η οποία μπορεί να προκληθεί από τις δοκιμές και τους ελέγχους που θα πραγματοποιηθούν, με εξαίρεση την περίπτωση που οι ζημιές αυτές είναι το αποτέλεσμα αμέλειας ή σκόπιμης κακόβουλης ενέργειας της ομάδας ελέγχου ασφάλειας δικτύου.

Άρθρο 18
Εφαρμογή

1. Ο πάροχος διαδικτύου πραγματοποιεί διαδικασία ελέγχου ασφάλειας δικτύου είτε αυτόβουλα, σε τακτά χρονικά διαστήματα, είτε ύστερα από αιτιολογημένο αίτημα της ΑΔΑΕ.

ΚΕΦΑΛΑΙΟ VII
ΔΙΑΔΙΚΑΣΙΑ ΑΠΟΤΙΜΗΣΗΣ ΚΙΝΔΥΝΩΝ

Άρθρο 19
Γενικά

1. Ως Διαδικασία Αποτίμησης Κινδύνων ορίζεται η διαδικασία εντοπισμού, ελέγχου και αξιολόγησης των τρωτών σημείων και απειλών ασφαλείας των πληροφοριακών και δικτυακών συστημάτων του παρόχου διαδικτύου σε ότι αφορά στην εμπιστευτικότητα και ακεραιότητα των δεδομένων και τη διαθεσιμότητα των παρεχόμενων υπηρεσιών.

2. Ειδικότερα για το τηλεπικοινωνιακό απόρρητο, η Διαδικασία Αποτίμησης Κινδύνων εστιάζεται στις απειλές που σχετίζονται με την προστασία των δεδομένων επικοινωνίας των χρηστών των υπηρεσιών ηλεκτρονικών επικοινωνιών.

3. Σκοπός της είναι να βοηθήσει τον πάροχο διαδικτύου να επιλέξει τις διαδικασίες και πρακτικές που ελαχιστοποιούν την πιθανότητα παραβίασης του απορρήτου επικοινωνιών των χρηστών καθώς και το κόστος εφαρμογής τους.

Άρθρο 20
Περιεχόμενο

1. Ο πάροχος διαδικτύου οφείλει να συγκροτεί Ομάδα Αποτίμησης Κινδύνων, η οποία θα αναλαμβάνει να αναλύει τους κινδύνους που υφίστανται για το απόρρητο επικοινωνιών των χρηστών. Συνιστάται η Ομάδα να περιλαμβάνει τόσο τεχνικό προσωπικό (προγραμματιστές, μηχανικούς ασφαλείας κτλ) όσο και ανώτερα στελέχη, ώστε η αποτίμηση να είναι ολοκληρωμένη και να λαμβάνει υπόψη όλες τις αναγκαίες πτυχές.

2. Η Ομάδα Αποτίμησης Κινδύνων οφείλει να συνέρχεται τουλάχιστον μια φορά κάθε 12 μήνες και να συντάσσει την Αναφορά Αποτίμησης Κινδύνων σύμφωνα με το άρθρο 21. Επιπλέον, συνιστάται η ομάδα να συνέρχεται όποτε παρουσιάζεται κάποιο σημαντικό θέμα ασφαλείας, όπως νέες απειλές, αλλαγή/ανανέωση τηλεπικοινωνιακού υλικού, ενεργοποίηση καινούργιας εφαρμογής λογισμικού, μεταξύ άλλων.

3. Ο πάροχος διαδικτύου οφείλει να ορίζει Υπεύθυνο Αποτίμησης Κινδύνων. Συνιστάται να είναι στέλεχος του παρόχου διαδικτύου και να μην συμμετέχει στην Ομάδα Αποτίμησης Κινδύνων. Ο Υπεύθυνος Αποτίμησης Κινδύνων οφείλει:

(α) Να ελέγχει την ποιότητα των εργασιών της Ομάδας Αποτίμησης Κινδύνων.

(β) Να ελέγχει την Αναφορά Αποτίμησης Κινδύνων και να την παραδίδει εγκαίρως στον Υπεύθυνο Ασφάλειας του παρόχου διαδικτύου.

4. Σε περίπτωση ανάθεσης του έργου σε τρίτο με σύμβασης υπεργολαβίας, η τελική ευθύνη της Διαδικασίας Αποτίμησης Κινδύνων παραμένει στον πάροχο διαδικτύου. Τυχόν αμέλεια του Υπευθύνου Αποτίμησης Κινδύνων συνεπάγεται κυρώσεις κατά του ιδίου αλλά και κατά του παρόχου διαδικτύου, ο οποίος εν τέλει είναι υπεύθυνος για την διασφάλιση του απορρήτου.

Άρθρο 21
Αναφορά Αποτίμησης Κινδύνων

1. Η Διαδικασία Αποτίμησης Κινδύνων οφείλει να περιγράφει λεπτομερώς και να ακολουθεί κατ' ελάχιστον τα παρακάτω βήματα:

(α) Καταγραφή των Πόρων Δεδομένων Επικοινωνιών: πρόκειται για την πλήρη καταγραφή όλων των πόρων που χρησιμοποιούνται για την παρακολούθηση, αποθήκευση, επεξεργασία, εξαγωγή, διαβίβαση, ανακοίνωση και δημοσιοποίηση δεδομένων επικοινωνίας. Συνιστάται επίσης η καταγραφή των μέτρων ασφαλείας που ισχύουν ήδη.

(β) Κατηγοριοποίηση των Πόρων Δεδομένων Επικοινωνιών: κάθε πόρος δεδομένων επικοινωνιών πρέπει να χαρακτηριστεί ως «κρίσιμος», «βασικός» ή «κανονικός» με κριτήριο τη σημασία ως προς το απόρρητο των δεδομένων επικοινωνιών που διαχειρίζεται ο κάθε πόρος.

(γ) Καταγραφή Ευπαθειών: για κάθε Πόρο Δεδομένων Επικοινωνιών πρέπει να καταγράφονται όλες οι ευπάθειες (αδυναμίες, ελαττώματα) που είναι δυνατόν να θέσουν σε κίνδυνο το απόρρητο επικοινωνιών των χρηστών.

(δ) Κατηγοριοποίηση Ευπαθειών: κάθε ευπάθεια που καταγράφηκε στο προηγούμενο βήμα οφείλει να ορισθεί με σαφήνεια και να χαρακτηρισθεί ως «κρίσιμη», «σημαντική» ή «δευτερεύουσα» με κριτήριο το πόσο επικίνδυνη είναι για τη διατήρηση του απορρήτου επικοινωνιών των χρηστών.

(ε) Καταγραφή Απειλών: για κάθε Πόρο Δεδομένων Επικοινωνιών πρέπει να καταγράφονται όλες οι απειλές που είναι δυνατόν να εκμεταλλευτούν μια ευπάθεια και να θέσουν σε κίνδυνο το απόρρητο επικοινωνιών των χρηστών.

(στ) Κατηγοριοποίηση Απειλών: κάθε απειλή που καταγράφηκε στο προηγούμενο βήμα οφείλει να ορισθεί με σαφήνεια και να χαρακτηρισθεί ως «κρίσιμη», «σημαντική» ή «δευτερεύουσα» με κριτήριο το πόσο επικίνδυνη είναι για τη διατήρηση του απορρήτου επικοινωνιών των χρηστών. Πρέπει να λαμβάνονται υπόψη τόσο τα αποτελέσματα μιας τέτοιας απειλής καθώς και η πιθανότητα να συμβεί.

(ζ) Ιεράρχηση Κινδύνου: πρόκειται για την ταξινόμηση όλων των συνδυασμών «Πόρος Δεδομένων Επικοινωνιών - Ευπάθεια - Απειλή» ως προς την κρισιμότητα του κινδύνου. Στο βήμα αυτό, οποιαδήποτε μεθοδολογία αποτίμησης και αν ακολουθείται, πρέπει να αναφέρεται ξεκάθαρα ποιοι συνδυασμοί παρουσιάζουν μεγαλύτερο κίνδυνο για τη διατήρηση του απορρήτου επικοινωνιών των χρηστών και ποιοι μικρότερο.

(η) Προτάσεις Αντιμετώπισης Κινδύνου: για κάθε συνδυασμό «Πόρος Δεδομένων Επικοινωνιών - Ευπάθεια - Απειλή» του προηγούμενου βήματος πρέπει να προτείνεται και να περιγράφεται λεπτομερώς τουλάχιστον μία λύση. Η λύση αυτή είναι πιθανόν να αφορά είτε συγκεκριμένα τεχνικά βήματα είτε πολιτικές - διαδικασίες αντιμετώπισης του κινδύνου. Για κάθε λύση συνιστάται επίσης να καθορίζονται το σκεπτικό, τα προτερήματα και μειονεκτήματά της έναντι των άλλων λύσεων, το πιθανό κόστος και ο χρονικός ορίζοντας υλοποίησής της. Ιδιαίτερη προσοχή πρέπει να δίνεται στις περιπτώσεις υψηλού κινδύνου.

(θ) Προτεινόμενη λύση: για κάθε συνδυασμό «Πόρος Δεδομένων Επικοινωνιών - Ευπάθεια - Απειλή» πρέπει να επιλέγεται μία λύση ανάμεσα σε αυτές που αναφέρθηκαν στο προηγούμενο βήμα (εφόσον οι λύσεις είναι περισσότερες από μία). Για αυτήν τη λύση πρέπει να αναφέρονται τόσο οι λόγοι που οδήγησαν στην επιλογή αυτή όσο και τον υπολειπόμενο κίνδυνο.

2. Η Αναφορά Αποτίμησης Κινδύνων οφείλει επίσης να αναφέρει τα μέλη της Ομάδας Αποτίμησης Κινδύνων, τον Υπεύθυνο Αποτίμησης Κινδύνων και την ημερομηνία δημιουργίας της.

ΚΕΦΑΛΑΙΟ VIII
ΕΛΕΓΧΟΣ ΚΑΙ ΕΠΟΠΤΕΙΑ

Άρθρο 22
Γενικά

1. Οι πολιτικές και οι διαδικασίες που ορίστηκαν στον κανονισμό αυτό αποτελούν μέρος της γενικότερης Πολιτικής Ασφάλειας του παρόχου διαδικτύου, όπως αυτή ορίστηκε στον «Κανονισμό για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές».

2. Κατά συνέπεια, η ΑΔΑΕ στα πλαίσια ελέγχου και εποπτείας που καθορίστηκαν στον «Κανονισμό για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές», μπορεί ανά πάσα στιγμή να προβεί σε έλεγχο του καθορισμού, επιβολής και σωστής λειτουργίας των πολιτικών που ορίστηκαν στον παρόντα Κανονισμό.

3. Σχετικά με τις λεπτομερείς διαδικασίες διενέργειας του ελέγχου καθώς και τις προβλεπόμενες διοικητικές κυρώσεις ισχύουν, κατ' αναλογία, τα αναγραφόμενα στον «Κανονισμό για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές».

Άρθρο 23
Πολιτική Ασφάλειας Περιμέτρου

1. Η ΑΔΑΕ μπορεί να διενεργεί αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου εφαρμόζει Πολιτική Ασφάλειας Περιμέτρου και ακολουθεί τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.

2. Ο πάροχος διαδικτύου υποχρεούται να παραδίδει στα στελέχη της ΑΔΑΕ την πιο πρόσφατη Πολιτική Ασφάλειας Περιμέτρου είτε κατά τη διάρκεια ελέγχου είτε κάθε φορά που πραγματοποιείται κάποια σημαντική αλλαγή σε αυτή. Επιπρόσθετα, ο πάροχος διαδικτύου υποχρεούται περιοδικά να αποστέλλει στην ΑΔΑΕ τις τελευταίες Φόρμες Καταγραφής Επισυνδέσεων.

3. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην Πολιτική Ασφάλειας Περιμέτρου. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος διαδικτύου οφείλει να προσαρμόζει την Πολιτική Ασφάλειας Περιμέτρου αναλόγως, εντός της προθεσμίας που θα ορίζεται από το κείμενο τροποποίησης.

Άρθρο 24
Πολιτική Διαχείρισης και Εγκατάστασης
Τηλεπικοινωνιακού Εξοπλισμού

1. Το εξουσιοδοτημένο προσωπικό του παρόχου διαδικτύου διενεργεί περιοδικούς ελέγχους προκειμένου να διαπιστώσει κατά πόσον τηρείται η Πολιτικής Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού στις διάφορες οργανικές μονάδες του παρόχου διαδικτύου. Σε όσες περιπτώσεις είναι δυνατό θα πρέπει να γίνεται χρήση αυτοματοποιημένων εργαλείων τα οποία π.χ. συλλέγουν και αναλύουν δεδομένα από αρχεία καταγραφής ή/και πραγματοποιούν εικονικές επιθέσεις στον εξοπλισμό του παρόχου διαδικτύου για διαπίστωση πιθανών κενών ασφαλείας. Η διαδικασία των περιοδικών ελέγχων θα πρέπει να έχει σχεδιαστεί με τέτοιο τρόπο έτσι ώστε να τελεί υπό την άμεση εποπτεία του Υπεύθυνου Ασφάλειας του παρόχου διαδικτύου.

2. Η ΑΔΑΕ διενεργεί αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου διατηρεί και εφαρμόζει επαρκή και ενημερωμένη Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού, η οποία συμφωνεί με τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.

3. Ο υπό έλεγχο πάροχος διαδικτύου οφείλει να παραδώσει στα στελέχη της ΑΔΑΕ την εν ενεργεία Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού καθώς και να παρέχει πρόσβαση στην έντυπη ή/και ηλεκτρονική καταγραφή των πράξεων που σχετίζονται με εγκατάσταση, απεγκατάσταση, αναβάθμιση, αλλαγή διαμόρφωσης του τηλεπικοινωνιακού εξοπλισμού του.

4. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος διαδικτύου οφείλει να προσαρμόζει την Πολιτική Διαχείρισης και Εγκατάστασης Τηλεπικοινωνιακού Εξοπλισμού αναλόγως.

Άρθρο 25
Πολιτική Αντιγράφων Ασφάλειας

1. Η ΑΔΑΕ μπορεί να διενεργεί αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου εφαρμόζει την Πολιτική Αντιγράφων Ασφάλειας και ακολουθεί τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.

2. Ο πάροχος διαδικτύου υποχρεούται να παραδίδει στα στελέχη της ΑΔΑΕ την πιο πρόσφατη Πολιτική Αντιγράφων Ασφάλειας είτε κατά τη διάρκεια ελέγχου είτε κάθε φορά που πραγματοποιείται κάποια σημαντική αλλαγή σε αυτή.

3. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην Πολιτική Αντιγράφων Ασφάλειας. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος διαδικτύου οφείλει να προσαρμόζει την Πολιτική Αντιγράφων Ασφάλειας αναλόγως, εντός της προθεσμίας που θα ορίζεται από το κείμενο τροποποίησης.

Άρθρο 26
Διαδικασία Χειρισμού Περιστατικών Ασφάλειας

1. Η ΑΔΑΕ μπορεί να διενεργεί αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου διατηρεί επαρκή και ενημερωμένη Δ.Χ.Π.Α. η οποία συμφωνεί με τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.

2. Ο υπό έλεγχο πάροχος διαδικτύου οφείλει να παραδώσει στα στελέχη της ΑΔΑΕ την τελευταία Δ.Χ.Π.Α. Η ΑΔΑΕ μπορεί επιπλέον να ζητήσει την ενεργοποίηση της διαδικασίας είτε για να διαπιστώσει την ετοιμότητα του παρόχου είτε για να διερευνήσει καταγγελθέντα περιστατικά.

3. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην Δ.Χ.Π.Α.. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος διαδικτύου οφείλει να προσαρμόζει τη Δ.Χ.Π.Α. αναλόγως.

Άρθρο 27
Διαδικασία Ελέγχου Ασφάλειας Δικτύου

1. Κατά τη διάρκεια ελέγχου ασφάλειας δικτύου, η ΑΔΑΕ μπορεί να διενεργήσει αυτοψία για να διαπιστώσει αν όντως τηρούνται οι διαδικασίες ελέγχου ασφάλειας δικτύου, και αν ο πάροχος διαδικτύου εφαρμόζει τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.

2. Κατά τη διάρκεια ελέγχου ασφάλειας δικτύου, οι εμπλεκόμενοι φορείς στη διαδικασία ελέγχου ασφάλειας δικτύου, οφείλουν να ενημερώσουν άμεσα την ΑΔΑΕ για οποιεσδήποτε αποκλίσεις ή παραβιάσεις της διαδικασίας ελέγχου ασφάλειας δικτύου.

3. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν τη διαδικασία ελέγχου ασφάλειας δικτύου. Μετά από κάθε τέτοιου είδους τροποποίηση, η πραγματοποίηση οποιουδήποτε νέου ελέγχου ασφάλειας δικτύου, οφείλει να είναι σύμφωνη με το νέο τροποποιημένο Κανονισμό.

Άρθρο 28
Διαδικασία Αποτίμησης Κινδύνων

1. Η ΑΔΑΕ μπορεί να διενεργεί αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου εφαρμόζει Διαδικασία Αποτίμησης Κινδύνων και ακολουθεί τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.

2. Ο υπό έλεγχο πάροχος διαδικτύου οφείλει να παραδώσει στα στελέχη της ΑΔΑΕ την τελευταία Αναφορά Αποτίμησης Κινδύνων η οποία οφείλει να είναι ενημερωμένη και σύμφωνη με την υπάρχουσα κατάσταση σε ότι αφορά στους κινδύνους παραβίασης του απορρήτου επικοινωνιών των χρηστών.

3. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην Διαδικασία Αποτίμησης Κινδύνων. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος διαδικτύου οφείλει να προσαρμόζει τη Διαδικασία Αποτίμησης Κινδύνων αναλόγως και να συγκαλεί την Ομάδα Αποτίμησης Κινδύνων εντός της προθεσμίας που θα ορίζεται από το κείμενο τροποποίησης.

ΚΕΦΑΛΑΙΟ IX
ΜΕΤΑΒΑΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 29
Μεταβατικές Διατάξεις

1. Όλοι οι πάροχοι διαδικτύου υποχρεούνται:

(α) Να ενημερώσουν ως προς την εφαρμοζόμενη πολιτική ασφάλειας την ΑΔΑΕ εντός έξι (6) μηνών από τη δημοσίευση του παρόντος.

(β) Να εφαρμόζουν την εγκριθείσα από την ΑΔΑΕ πολιτική ασφάλειας εντός ενός (1) έτους από την έγκρισή της.

ΚΕΦΑΛΑΙΟ X
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 30
Έναρξη Ισχύος

1. Ο παρών Κανονισμός τίθεται σε ισχύ από την ημερομηνία δημοσίευσής του στην Εφημερίδα της Κυβερνήσεως.

Ο παρών Κανονισμός να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Αθήνα, 14 Ιανουαρίου 2005

Ο Πρόεδρος
ΑΝΔΡΕΑΣ ΛΑΜΠΡΙΝΟΠΟΥΛΟΣ

Αριθ. 634 α (3)

Κανονισμός για τη Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου.

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ
ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΑΔΕΑ)

Έχοντας υπόψη :

α. Το Ν. 3115/27-02-2003, άρθρο 1, παραγρ. 1,

β. Το Ν. 3115/27-02-2003, άρθρο 6, παραγρ. 1

γ. Ότι εκ της αποφάσεως δεν προκύπτει δαπάνη για το δημόσιο

δ. Τη σχετική εισήγηση της Υπηρεσίας, αποφάσισε:

κατά τη συνεδρίασή της την 10η Νοεμβρίου 2004, την έγκριση του παρακάτω Κανονισμού για τη Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου.

ΚΕΦΑΛΑΙΟ I
ΣΚΟΠΟΣ - ΟΡΙΣΜΟΙ

Άρθρο 1
Σκοπός - Πεδίο Εφαρμογής

1. Σκοπός του παρόντος Κανονισμού είναι:

(α) Η διασφάλιση του απορρήτου των εφαρμογών στο Διαδίκτυο και των χρηστών τους.

(β) Η ασφάλεια των παρόχων υπηρεσίας εφαρμογής ως προς τις προσφερόμενες υπηρεσίες και εφαρμογές.

(γ) Η θέσπιση των υποχρεώσεων των εν λόγω παρόχων αναφορικά με την ασφάλεια και το απόρρητο των εφαρμογών Διαδικτύου και των χρηστών.

(δ) Ο έλεγχος στους εν λόγω παρόχους σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

2. Στις διατάξεις του παρόντος Κανονισμού εμπίπτουν όλοι οι Τηλεπικοινωνιακοί Φορείς Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα:

(α) Πάροχοι σταθερής και κινητής πρόσβασης στο Διαδίκτυο

(β) Πάροχοι Διαδικτυακών υπηρεσιών, υπηρεσιών προστιθέμενης αξίας και υπηρεσίας εφαρμογών.

Άρθρο 2
Ορισμοί

Για την εφαρμογή του παρόντος Κανονισμού ισχύουν οι ορισμοί του «Κανονισμού για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές» της ΑΔΑΕ, που επαναλαμβάνονται για πληρότητα. Επιπρόσθετα, οι ακόλουθοι όροι έχουν την έννοια που τους αποδίδεται κατωτέρω:

Ασύμμετρη Κρυπτογραφία - στηρίζεται στη χρήση ενός ζευγαριού κλειδιών, ενός ιδιωτικού και ενός δημόσιου. Όταν η κρυπτογράφηση γίνεται με το ένα κλειδί, η αποκρυπτογράφηση γίνεται με το άλλο. Είναι γνωστή και ως Κρυπτογραφία Δημόσιου Κλειδιού.

Ακεραιότητα - είναι ιδιότητα της διαδικασίας ασφάλειας με την οποία ελέγχεται αν τα δεδομένα έχουν τροποποιηθεί ή καταστραφεί κατά μη εξουσιοδοτημένο τρόπο.

Δεδομένα Θέσης - τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.

Δεδομένα Κίνησης - τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της.

Διαδικτυακές Επικοινωνίες - Υπηρεσίες ηλεκτρονικών επικοινωνιών όπου το δίκτυο ηλεκτρονικών επικοινωνιών είναι δίκτυο μετάδοσης δεδομένων και φωνής με πακετομεταγωγή το οποίο είτε έχει τη μορφή ενδοδικτύου (Intranet) είτε είναι ολόκληρο το Διαδίκτυο (Internet).

Δίκτυο Ηλεκτρονικών Επικοινωνιών - τα συστήματα μετάδοσης και, κατά περίπτωση, ο εξοπλισμός μεταγωγής ή δρομολόγησης και οι λοιποί πόροι που επιτρέπουν τη μεταφορά σημάτων, με τη χρήση καλωδίου, ραδιοσημάτων, οπτικού ή άλλου ηλεκτρομαγνητικού μέσου, συμπεριλαμβανομένων των δορυφορικών δικτύων, των σταθερών (μεταγωγής δεδομένων μέσω κυκλωμάτων και πακετομεταγωγής, συμπεριλαμβανομένου του Διαδικτύου) και κινητών επίγειων δικτύων, των συστημάτων ηλεκτρικών καλωδίων, εφόσον χρησιμοποιούνται για τη μετάδοση σημάτων, των δικτύων που χρησιμοποιούνται για ραδιοτηλεοπτικές εκπομπές, καθώς και των δικτύων καλωδιακής τηλεόρασης, ανεξάρτητα από το είδος των μεταφερόμενων πληροφοριών.

Εμπιστευτικότητα - η ιδιότητα της διαδικασίας ασφάλειας με την οποία αποτρέπεται η διάθεση ή η αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένα άτομα, οντότητες ή διεργασίες.

Εξουσιοδότηση - η διαδικασία χορήγησης δικαιώματος πρόσβασης ή χρήσης μιας υπηρεσίας ή πληροφοριών, με βάση την έγκυρη ταυτότητα. Η εξουσιοδότηση χορηγείται από την οντότητα που ελέγχει τον πόρο για τον οποίο ζητάτε η πρόσβαση.

Επαλήθευση Ταυτότητας (Authentication) - αναφέρεται στις αυτοματοποιημένες και τυποποιημένες μεθόδους για την πιστοποίηση της ταυτότητας του χρήστη στο Διαδίκτυο. Αναφέρεται και ως αυθεντικοποίηση.

Ιός (virus) - Ως ιός περιγράφεται ένα κομμάτι κώδικα λογισμικού το οποίο εισβάλλει σε ένα υπολογιστικό σύστημα με σκοπό να προκαλέσει ανεπιθύμητα αποτελέσματα, όπως καταστροφή δεδομένων χρήστη, άρνηση υπηρεσίας (denial-of-service), παραβίαση του συστήματος ασφαλείας του συστήματος κτλ. Κύριο χαρακτηριστικό του είναι το γεγονός ότι μεταδίδεται μεταξύ των υπολογιστικών συστημάτων με τη μορφή εκτελέσιμων προγραμμάτων (executables), εγγραφών συστήματος (system or boot records) και μακρο-εντολών (macros). Οι ιοί είναι δυνατόν να επιτεθούν κατά προσωπικών υπολογιστών, servers, routers κτλ.

Κλειδί Κρυπτογράφησης - μια σειρά από bits συγκεκριμένου μήκους που χρησιμοποιείται για να κρυπτογραφήσει ή να αποκρυπτογραφήσει τα δεδομένα σε έναν αλγόριθμο κρυπτογράφησης.

Λογισμικό Προστασίας από Ιούς (anti-virus software) - Πρόκειται για μια κατηγορία εφαρμογών λογισμικού που αποσκοπεί στην ανίχνευση και απομάκρυνση ιών που έχουν προσβάλλει ένα υπολογιστικό σύστημα.

Μη Αποποίηση Ευθύνης - εξασφαλίζει ότι οι συναλλασσόμενοι σε εφαρμογές και υπηρεσίες Διαδικτύου που προσφέρονται είτε από πάροχους διαδικτύου είτε από πάροχους υπηρεσίας εφαρμογής δεν μπορούν να αρνηθούν τη συμμετοχή τους στη συναλλαγή.

Παροχή Δικτύου Διαδικτυακών Επικοινωνιών - η σύσταση, η λειτουργία, ο έλεγχος και η διάθεση τέτοιου δικτύου.

Πάροχος Δικτύου Διαδικτυακών Επικοινωνιών (Internet Service Provider) - Η επιχείρηση ή το νομικό πρόσωπο που παρέχει δίκτυο διαδικτυακών επικοινωνιών ή/και το νομικό πρόσωπο που παρέχει στο προσωπικό του την απαραίτητη δικτυακή υποδομή για χρήση διαδικτυακών επικοινωνιών στα πλαίσια της εργασίας του. Για τις ανάγκες του παρόντος ο πάροχος δικτύου διαδικτυακών επικοινωνιών θα αναφέρεται στη συνέχεια του κειμένου ως «πάροχος διαδικτύου».

Πάροχος Υπηρεσίας Εφαρμογής (Application Service Provider) - μία οντότητα (οργανισμός, εταιρεία κτλ), η οποία διαθέτει εφαρμογές λογισμικού (software), υλική υποδομή (hardware) και δικτυακή υποδομή, προκειμένου να παρέχει υπηρεσίες και εφαρμογές στον πάροχο δικτύου διαδικτυακών επικοινωνιών και τους χρήστες του.

Πολιτική ασφάλειας - Το σύνολο τεχνικών, οργανωτικών και κανονιστικών μέτρων, τα οποία εφαρμόζονται από πάροχο διαδικτύου και αποβλέπουν στη διασφάλιση του απορρήτου και γενικά στην ασφαλή λειτουργία των δικτύων διαδικτυακών επικοινωνιών.

Προσδιορισμός ταυτότητας - αναφέρεται σε λιγότερο τυποποιημένες μεθόδους (σε σχέση με τη διαδικασία επαλήθευσης ταυτότητας) για την πιστοποίηση της φύσης του χρήστη, που είναι συνήθως μη αυτόματες και απαιτούν ανθρώπινη παρέμβαση.

Προστασία του απορρήτου - η απαγόρευση της ακρόασης, της παγίδευσης, της αποθήκευσης, της επεξεργασίας, της ανακοίνωσης, της δημοσιοποίησης ή άλλου τύπου υποκλοπής ή παρακολούθησης της τηλεπικοινωνίας και των δεδομένων επικοινωνίας από άλλα πρόσωπα, χωρίς τη συγκατάθεσή τους, εξαιρουμένων των νόμιμα εξουσιοδοτημένων.

Συγκατάθεση του Χρήστη ή του Συνδρομητή - η συγκατάθεση του προσώπου που αφορούν τα δεδομένα, κατά την έννοια της οδηγίας 95/46/ΕΚ.

Συμμετρική Κρυπτογραφία - η κρυπτογράφηση και αποκρυπτογράφηση πραγματοποιούνται με ένα κλειδί.

Ταυτότητα - είναι οι πληροφορίες που προσδιορίζουν το χρήστη με μοναδικό τρόπο.

Υπεργολάβος - όπως αυτός ορίζεται από την υπάρχουσα νομοθεσία.

Υπηρεσία Προστιθέμενης Αξίας - υπηρεσία μη τηλεπικοινωνιακή η οποία μπορεί να παρέχεται ή να υποστηρίζεται από δίκτυο διαδικτυακών επικοινωνιών.

Υπηρεσίες Ηλεκτρονικών Επικοινωνιών - οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις. Στις υπηρεσίες ηλεκτρονικών επικοινωνιών δεν περιλαμβάνονται υπηρεσίες παροχής ή ελέγχου περιεχόμενου που μεταδίδεται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και υπηρεσίες της κοινωνίας της πληροφορίας, όπως αυτές ορίζονται στην παράγραφο 2 του άρθρου 2 του ΠΔ39/2001 (Α'28), και που δεν αφορούν, εν όλω ή εν μέρει, τη μεταφορά σημάτων σε δίκτυα επικοινωνιών.

Χρήστης: κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας.

Χρήστης Παρόχου: κάθε φυσικό πρόσωπο που εργάζεται στην επιχείρηση ή το νομικό πρόσωπο που παρέχει στο προσωπικό του την απαραίτητη δικτυακή υποδομή για χρήση διαδικτυακών επικοινωνιών στα πλαίσια της εργασίας του.

ΚΕΦΑΛΑΙΟ ΙΙ
ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΧΡΗΣΤΗ ΔΙΑΔΙΚΤΥΟΥ

Άρθρο 3
Σκοπός, Κανόνες και Συνθήκες

1. Ο σκοπός της πολιτικής ασφάλειας χρήστη Διαδικτύου είναι να ορίσει τους κανόνες και τις απαιτήσεις ασφάλειας για τη χρήση του Διαδικτύου ως ασφαλές μέσο για τη μετάδοση ευαίσθητων πληροφοριών και να διασφαλίσει την χρήση του.

2. Οι πιο κάτω κανόνες και συνθήκες αφορούν όλους τους χρήστες που χρησιμοποιούν το Διαδίκτυο ή έχουν κάποιο σημείο προσαρμογής σε αυτό, με σκοπό τη μετάδοση πληροφοριών. Η πολιτική αυτή δεν καλύπτει την προστασία υποδομών τοπικών δεδομένων ή τοπικών δικτύων (LAN κτλ).

3. Μια ολοκληρωμένη υλοποίηση Διαδικτυακής επικοινωνίας θα πρέπει να περιλαμβάνει επαρκείς μεθόδους κρυπτογράφησης (encryption), χρησιμοποίηση επαλήθευσης ή προσδιορισμού ταυτότητας (authentication or identification) από τους χρήστες και ένα σχέδιο διαχείρισης που θα ενσωματώνει αποδοτικές μεθόδους διαχείρισης κλειδιών και κωδικών πρόσβασης. Πιο συγκεκριμένα:

(α) Οι μέθοδοι που εφαρμόζονται από τους χρήστες θα πρέπει να περιλαμβάνουν μια μέθοδο κρυπτογράφησης και τουλάχιστον μία μέθοδο επαλήθευσης και προσδιορισμού ταυτότητας. Αυτές οι μέθοδοι πρέπει να είναι αρκετά γενικές και ανοικτές ώστε να παρέχουν μέγιστη προσαρμοστικότητα από την πλευρά του χρήστη και των εφαρμογών, μέσα όμως σε κάποια όρια ασφάλειας και εύκολης διαχείρισης.

(β) Οι τεχνικές θα πρέπει να παρέχουν στο χρήστη τη δυνατότητα να αποδεικνύει ότι είναι αυτός που δηλώνεται και να οργανώνουν έτσι τα δεδομένα προς μετάδοση ώστε να αποφεύγεται η ανάρμοστη γνωστοποίηση ή τροποποίηση των δεδομένων κατά τη μετάδοσή τους. Επομένως, τεχνικές επαλήθευσης και προσδιορισμού της ταυτότητας του χρήστη θα πρέπει να συνυπάρχουν με τεχνικές κρυπτογράφησης και μετάδοσης δεδομένων ώστε να εγγυηθούν ότι τα δεδομένα θα μεταφερθούν με ασφαλή τρόπο και ότι μόνο οι εξουσιοδοτημένοι χρήστες θα μπορέσουν να τα διαβάσουν.

(γ) Υπάρχουν περιπτώσεις που «σταθεροί» κωδικοί πρόσβασης δεν επαρκούν, αλλά χρειάζεται ένα είδος δυναμικής πιστοποίησης των δεδομένων. Μια σειρά από διαφορετικές τεχνολογίες μπορούν να παρέχουν ένα είδος δυναμικής πιστοποίησης, όπως γεννήτριες δυναμικών κωδικών, τεχνικές βασισμένες στην κρυπτογραφία, καθώς και ψηφιακές υπογραφές και πιστοποιητικά.

(δ) Οι τεχνικές προσδιορισμού των κωδικών πρόσβασης παρέχουν ένα επίπεδο ασφάλειας. Η δυσκολία ανίχνευσης των κωδικών αυτών από τρίτα άτομα καθώς και ο τρόπος που αυτοί προστατεύονται καθορίζουν εμμέσως την ισχύ της διαδικασίας επαλήθευσης της ταυτότητας του χρήστη.

4. Οι χρήστες δεν θα πρέπει να δίνουν το λογαριασμό πρόσβασης καθώς και τους αντίστοιχους κωδικούς που έχουν σε άλλα μη εξουσιοδοτημένα άτομα.

5. Οι χρήστες δεν θα πρέπει να αλλάζουν χαρακτηριστικά των συστημάτων λογισμικού ή υλικού, καθώς και να μην εγκαθιστούν προγράμματα σε υπολογιστές ή στο δίκτυο που εν γνώσει τους μπορεί να προκαλέσουν ζημιές ή να δημιουργήσουν υπερβολικό φορτίο στο υπολογιστικό σύστημα ή στο δίκτυο.

6. Οι χρήστες πρέπει να συμμορφώνονται με τον τρόπο χρήσης του ηλεκτρονικού τους ταχυδρομείου όπως προσδιορίζεται από τους παρόχους διαδικτύου και το περιβάλλον εργασίας τους. Μπορεί να υπάρχουν κανόνες που να ορίζουν τόσο τη συμπεριφορά των χρηστών όσο και τις απαιτήσεις των εφαρμογών και των εξυπηρετητών ηλεκτρονικού ταχυδρομείου.

(α) Απαραίτητη θεωρείται η εξέταση των εισερχόμενων μηνυμάτων για ιούς και κακόβουλα δεδομένα

(β) Οι εξυπηρετητές (servers) του ηλεκτρονικού ταχυδρομείου μπορεί να είναι αρχικοποιημένοι ώστε κάθε μήνυμα να υπογράφεται χρησιμοποιώντας την ψηφιακή υπογραφή του αποστολέα, να απαγορεύουν την αποστολή μηνυμάτων σε μη κατάλληλους προορισμούς και να ανιχνεύουν τη χρήση με κατάλληλα προγράμματα για αποστολή / παραλαβή μηνυμάτων.

(γ) Οι χρήστες θα πρέπει να συμμορφώνονται με τους κανόνες ασφάλειας που ορίζονται από τους παρόχους διαδικτύου, ύστερα από ενημέρωσή τους από τον πάροχο διαδικτύου σχετικά με αυτούς τους κανόνες. Οι χρήστες δηλώνουν τη συμμόρφωσή τους με σαφή, ατελή και εύκολα προσβάσιμο τρόπο, είτε ενυπόγραφα είτε ηλεκτρονικά. Οι κανόνες αυτοί μπορεί να περιέχουν περιορισμούς ως προς το υλικό που θα μεταδώσουν, και να εξασφαλίζουν τη μη παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας, καθώς και τη μη εξουσιοδοτημένη πρόσβαση σε δικτυακούς πόρους.

(δ) Οι χρήστες δεν θα πρέπει να δημοσιοποιούν υλικό σε ηλεκτρονικούς τόπους, news groups ή mail lists, το οποίο είναι παράνομο, ή όχι κατάλληλο (π.χ. να στέλνουν electronic junk mail ή chain letters).

ΚΕΦΑΛΑΙΟ III
ΠΟΛΙΤΙΚΗ ΟΡΘΗΣ (ΔΕΟΝΤΟΛΟΓΙΚΗΣ) ΣΥΜΠΕΡΙΦΟΡΑΣ ΧΡΗΣΤΗ

Άρθρο 4
Σκοπός και πεδίο εφαρμογής της πολιτικής ορθής συμπεριφοράς

1. Η ανάπτυξη της επικοινωνίας μέσω Διαδικτύου και συναφών υπηρεσιών είναι τόσο προς όφελος των παρόχων διαδικτύου και υπηρεσίας εφαρμογής όσο και προς όφελος των χρηστών. Αφενός διότι θα οδηγήσουν στην επιχειρηματική ανάπτυξη των παρόχων αυτών, αφετέρου διότι οι παρεχόμενες υπηρεσίες εξυπηρετούν τον χρήστη. Προϋπόθεση της ανάπτυξης και διάδοσής τους είναι να διέπονται από Κανόνες Δεοντολογίας. Ενδεικτικά θα μπορούσαμε να αναφέρουμε τους κανόνες (Netiquette) που ορίζονται από την παγκόσμια κοινότητα του Διαδικτύου IETF.

2. Για την επιτυχία του ως άνω σκοπού θα πρέπει οι κανόνες αυτοί να γίνουν αποδεκτοί από όλους ανεξαιρέτως τους εμπλεκόμενους στις δικτυακές επικοινωνίες, δηλαδή τους χρήστες, τους χρήστες παρόχου και τους παρόχους επικοινωνιακών συστημάτων και εφαρμογών.

3. Η εφαρμογή των κανόνων αυτών σε επίπεδο φυσικού ή νομικού προσώπου συνιστά την πολιτική ορθής συμπεριφοράς του εν λόγω προσώπου.

Άρθρο 5
Πολιτική ορθής συμπεριφοράς παρόχων

1. Οι πάροχοι διαδικτύου είναι απαραίτητο να δίνουν το παράδειγμα σε κάθε επιχειρηματικό τους βήμα, και κάθε επιχειρηματική τους πράξη να είναι νόμιμη, ειλικρινής και να διέπεται από διαφάνεια.

2. Ο πάροχος διαδικτύου και οι χρήστες παρόχου θα πρέπει να προσπαθούν να διαφυλάσσουν τους κανόνες ορθής συμπεριφοράς και να απαντούν άμεσα σε τυχόν ερωτήματα χρηστών.

3. Ο πάροχος διαδικτύου θα πρέπει να προσπαθήσει να αυξήσει την εμπιστοσύνη των χρηστών στις παρεχόμενες εφαρμογές εφαρμόζοντας τους κανόνες της καθημερινής ορθής συμπεριφοράς και στο Διαδίκτυο.

4. Ο πάροχος διαδικτύου είναι υποχρεωμένος να καταγγέλλει άμεσα στην ΑΔΑΕ περιπτώσεις μη ορθής συμπεριφοράς μέσω των προσφερόμενων εφαρμογών που εμπίπτουν στην αντίληψή του όπως ορίζει κάθε φορά η ισχύουσα νομοθεσία.

5. Σε περιπτώσεις όπου η νομοθεσία αδυνατεί να επιβάλει όρους και κανόνες τότε η πολιτική ορθής συμπεριφοράς του παρόχου διαδικτύου θα πρέπει πάντοτε να διαφυλάσσει το χρήστη.

6. Η πολιτική ορθής συμπεριφοράς αποτελεί έννοια με ευρεία φιλοσοφική διάσταση και ως εκ τούτου καθίσταται δύσκολη η πλήρης καταγραφή της. Εν τούτοις, κάθε πάροχος διαδικτύου οφείλει να συμπεριλαμβάνει επίσημες αναφορές σε αυτήν σε κατάλληλα σημεία των επίσημων εγγράφων του (π.χ. γενικές αρχές λειτουργίας) όσο και στο υλικό που διανέμει στους χρήστες των διαδικτυακών υπηρεσιών του.

Άρθρο 6
Πολιτική ορθής συμπεριφοράς χρηστών

1. Οι χρήστες είναι υποχρεωμένοι να χρησιμοποιούν τις εφαρμογές, όπως αυτές παρέχονται από τον εκάστοτε πάροχο διαδικτύου, έχοντας υπόψη τους ότι οι κατά την κρατούσα αντίληψη κανόνες ορθής συμπεριφοράς, πρέπει να διαφυλάσσονται και κατά τη χρήση των εφαρμογών αυτών.

2. Σε κάθε περίπτωση που υποπίπτει στην αντίληψη του χρήστη μη ορθή συμπεριφορά και χρήση των εφαρμογών, είναι υποχρεωμένος να ειδοποιεί άμεσα τον πάροχο διαδικτύου ή και να καταγγέλλει το περιστατικό στις αρμόδιες υπηρεσίες.

3. Ο χρήστης πρέπει να κατανοήσει ότι είναι υπεύθυνος για κάθε πράξη του στο Διαδίκτυο. Σε περιπτώσεις όπου ο χρήστης χρησιμοποιεί το Διαδίκτυο και τις παρεχόμενες εφαρμογές για εκβιασμό, αποστολή μηνυμάτων ρατσιστικού ή προσβλητικού περιεχομένου κ.ο.κ, ο χρήστης διώκεται βάσει της υπάρχουσας νομοθεσίας.

Άρθρο 7
Ανήθικη συμπεριφορά

1. Οι πάροχοι διαδικτύου, οι χρήστες και οι χρήστες παρόχου θα πρέπει να αποφεύγουν κάθε είδους ανήθικη συμπεριφορά μέσω εφαρμογών Διαδικτύου.

2. Υπογραμμίζεται ότι η ανήθικη και παράνομη συμπεριφορά μέσω διαδικτυακών εφαρμογών δεν διαχωρίζεται νομικά από τις κανονικές περίπτωσης ανήθικης συμπεριφοράς, όπως αυτές προβλέπονται από την νομοθεσία.

3. Κάθε περίπτωση εκβιασμού, λιβελογραφίας, συκοφαντικής δυσφήμισης, ρατσιστικής μεταχείρισης, παιδοφιλίας, παρακολούθησης ή διαρροής απόρρητων πληροφοριών κ.ο.κ. καλύπτεται νομικά από την υπάρχουσα νομοθεσία, η οποία ισχύει και για τις περιπτώσεις στις οποίες χρησιμοποιήθηκαν διαδικτυακές επικοινωνίες και εφαρμογές. Ειδικά υπογραμμίζεται η περίπτωση όπου ο πάροχος διαδικτύου ή οι χρήστες παρόχου χρησιμοποιούν παράνομα και ανήθικα την προσφερόμενη στον χρήστη υπηρεσία.

ΚΕΦΑΛΑΙΟ IV
ΧΡΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΑΛΓΟΡΙΘΜΩΝ

Άρθρο 8
Κρυπτογράφηση

1. Η κρυπτογράφηση έχει βασικό σκοπό να διασφαλίσει την εμπιστευτικότητα, την ακεραιότητα και τη μη-αποποίηση ευθύνης στις συναλλαγές και τις επικοινωνίες μέσω Διαδικτύου, τα οποία και αποτελούν αναπόσπαστα στοιχεία της ιδιωτικότητας του χρήστη.

2. Οι πάροχοι διαδικτύου οφείλουν να εφαρμόζουν αλγόριθμους και τεχνικές κρυπτογράφησης τόσο στα συστήματα μετάδοσης δεδομένων που χρησιμοποιούν όσο και στις εφαρμογές και τις υπηρεσίες του Διαδικτύου που παρέχουν. Σχετικά με το τελευταίο, ενδεικτικά και όχι περιοριστικά αναφέρονται οι υπηρεσίες ηλεκτρονικού εμπορίου, οι τραπεζικές συναλλαγές μέσω Διαδικτύου και το ηλεκτρονικό ταχυδρομείο.

3. Σχετικά με τα συστήματα μετάδοσης, οι πάροχοι διαδικτύου είναι υποχρεωμένοι να ακολουθούν τα διεθνή πρότυπα ανάλογα με τη τεχνολογία μετάδοσης που ακολουθείται. Οι πάροχοι διαδικτύου είναι υποχρεωμένοι να ενημερώνουν την ΑΔΑΕ ως προς τις τεχνικές κρυπτογράφησης που ακολουθούν.

4. Ανεξάρτητα από το πεδίο στο οποίο εφαρμόζονται τεχνικές κρυπτογράφησης, το επίπεδο της κρυπτογράφησης πρέπει να είναι τέτοιο ώστε να εξασφαλίζει ότι η παραβίασή της δεν είναι δυνατή (σε λογικό χρόνο και με λογικούς υπολογιστικούς πόρους). Το επίπεδο της κρυπτογράφησης εκφράζεται συνήθως από το μέγεθος του κλειδιού κρυπτογράφησης. Στη γενική περίπτωση όσο μεγαλύτερο είναι το μήκος του κλειδιού τόσο δυσκολότερη γίνεται η παραβίαση της κρυπτογράφησης. Η ΑΔΑΕ θα εκδίδει τεχνικές οδηγίες και συστάσεις που θα καθορίζουν το μήκος του κλειδιού ανά πεδίο κρυπτογράφησης.

5. Ανεξάρτητα από το πεδίο στο οποίο εφαρμόζονται τεχνικές κρυπτογράφησης, οι αλγόριθμοι κρυπτογράφησης που θα χρησιμοποιούνται θα πρέπει να είναι οι ευρέως αποδεκτοί αλγόριθμοι. Ενδεικτικά και όχι περιοριστικά αναφέρονται οι αλγόριθμοι RSA, Diffie-Hellman και ElGamal για την ασύμμετρη κρυπτογραφία και οι 3DES (Data Encryption Standard), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish και CAST για τη συμμετρική κρυπτογραφία.

Άρθρο 9
Ασφάλεια Εφαρμογών Διαδικτύου

1. Για την ασφάλεια και τη διασφάλιση του απορρήτου των εφαρμογών Διαδικτύου έχουν αναπτυχθεί διάφορα πρωτόκολλα και εφαρμογές που βασίζονται στις γενικές αρχές της κρυπτογράφησης. Ανάλογα με τον τύπο εφαρμογής Διαδικτύου έχουν προταθεί και προτυποποιηθεί συγκεκριμένα πρωτόκολλα.

2. Οι πάροχοι υπηρεσίας εφαρμογής οφείλουν να κάνουν χρήση των ευρέως αποδεκτών τεχνικών και πρωτόκολλων ασφάλειας των εφαρμογών Διαδικτύου. Ενδεικτικά και όχι περιοριστικά αναφέρονται τα ακόλουθα πρωτόκολλα ανά τύπο εφαρμογής:

(α) Για εφαρμογές Παγκόσμιου Ιστού (WWW) (π.χ. ηλεκτρονικό εμπόριο, τραπεζικές συναλλαγές μέσω Διαδικτύου) χρησιμοποιούνται τα πρωτόκολλα Secure Sockets Layer (SSL) και Secure HTTP (S-HTTP). Εξασφαλίζουν αυθεντικοποίηση, εμπιστευτικότητα και ακεραιότητα στην ανταλλαγή δεδομένων μεταξύ στοιχείων του παγκόσμιου ιστού (φυλλομετρητές και εξυπηρετητές).

(β) Για εφαρμογές ηλεκτρονικού ταχυδρομείου (e-mail) χρησιμοποιούνται τα πρωτόκολλα S/MIME και PEM (Privacy Enhanced Mail), τα οποία εν ολίγοις κάνουν χρήση ψηφιακών υπογραφών και κρυπτογράφησης στα μεταδιδόμενα ηλεκτρονικά μηνύματα. Η εφαρμογή PGP (Pretty Good Privacy) χρησιμοποιείται για παρόμοιο σκοπό.

(γ) Το πρωτόκολλο SET (Secure Electronic Transaction) χρησιμοποιείται για ηλεκτρονικές πληρωμές μέσω πιστωτικών καρτών.

3. Δεδομένου ότι νέα πρωτόκολλα και τεχνολογίες θα ανακύπτουν με την πρόοδο της επιστήμης των υπολογιστών, η ΑΔΑΕ θα εκδίδει τεχνικές οδηγίες και συστάσεις προς τους πάροχους διαδικτύου σχετικά με αυτά τα νέα πρωτόκολλα και τις τεχνολογίες. Οι πάροχοι διαδικτύου είναι υποχρεωμένοι να ακολουθούν τα εκάστοτε ευρέως χρησιμοποιούμενα πρωτόκολλα και τεχνολογίες, είτε αυτόβουλα είτε έπειτα από έλεγχο και αντίστοιχη οδηγία από την ΑΔΑΕ.

ΚΕΦΑΛΑΙΟ V
ΧΡΗΣΗ ΚΩΔΙΚΩΝ ΑΣΦΑΛΕΙΑΣ (PASSWORDS)

Άρθρο 10
Ανάγκη ύπαρξης πολιτικής κωδικών ασφάλειας

1. Οι κωδικοί ασφάλειας αποτελούν ένα από τα σημαντικότερα πεδία της ασφάλειας των επικοινωνιών. Αποτελούν την τελευταία γραμμή άμυνας ενάντια σε αυτούς που θα προσπαθήσουν να επιβουλευθούν ένα δίκτυο δεδομένων, δημόσιο ή ιδιωτικό, ή ένα υπολογιστικό σύστημα.

2. Τα παραπάνω καθίστανται ακόμα πιο σημαντικά στις ακόλουθες περιπτώσεις:

(α) Στην περίπτωση που ο κωδικός ασφάλειας αφορά χρήστη παρόχου ο οποίος συνδέεται με τα συστήματα του παρόχου διαδικτύου από απόσταση, μέσω Διαδικτύου.

(β) Στην περίπτωση που ο κωδικός ασφάλειας αφορά χρήστη παρόχου ο οποίος αποκτά πρόσβαση από σύστημα του παρόχου διαδικτύου προς το Διαδίκτυο.

Και στις δύο περιπτώσεις ένας ακατάλληλος κωδικός ασφάλειας δύναται να οδηγήσει σε απώλεια σημαντικών δεδομένων καθώς και σε γενικότερη δυσλειτουργία των συστημάτων του παρόχου διαδικτύου.

3. Συνεπώς κάθε πάροχος διαδικτύου θα πρέπει να διαθέτει και να επιβάλλει κανόνες αναφορικά με τους κωδικούς ασφάλειας ούτως ώστε:

(α) Να δημιουργούνται συμπαγείς κωδικοί.

(β) Να προστατεύονται οι ως άνω κωδικοί.

(γ) Να μεταβάλλονται συχνά οι ως άνω κωδικοί.

4. Η πολιτική αυτή θα πρέπει να εφαρμόζεται από όλους τους χρήστες και χρήστες παρόχου, οι οποίοι διαθέτουν λογαριασμό με πρόσβαση από και προς το Διαδίκτυο και ιδιαίτερα αν χειρίζονται ευαίσθητα, μη διαθέσιμα στο κοινό, δεδομένα.

Άρθρο 11
Δημιουργία και Διαχείριση κωδικών ασφάλειας

1. Της εφαρμογής μιας πολιτικής δημιουργίας και διαχείρισης κωδικών ασφάλειας σε έναν πάροχο διαδικτύου προηγείται ο διαχωρισμός των συστημάτων σε αυτά που χρειάζονται προστασία μέσω κωδικών ασφάλειας και σε αυτά που διατίθενται προς ελεύθερη πρόσβαση.

2. Προκειμένου οι χρήστες και χρήστες παρόχου να χρησιμοποιήσουν ένα εταιρικό δίκτυο ή υπολογιστικό σύστημα το οποίο προστατεύεται, θα πρέπει να διαθέτουν «όνομα χρήστη» (login name) και κατάλληλο κωδικό ασφάλειας (password). Ως εκ τούτου η πολιτική κωδικών ασφάλειας περιλαμβάνει:

(α) Περιγραφή των κανόνων σύμφωνα με τους οποίους γίνεται η δημιουργία των ονομάτων χρηστών (user names)

(β) Περιγραφή των κανόνων σύμφωνα με τους οποίους γίνεται η δημιουργία των κωδικών ασφάλειας (passwords).

(γ) Περιγραφή των διαδικασιών σύμφωνα με τις οποίες διανέμεται σε κάθε χρήστη ή χρήστη παρόχου το αντίστοιχο όνομα χρήστη καθώς και ο κωδικός ασφάλειας.

(δ) Περιγραφή των κανόνων σύμφωνα με τους οποίους επιτυγχάνεται η τακτική αλλαγή των κωδικών ασφάλειας και η εν γένει διαχείρισή τους.

(ε) Περιγραφή των κανόνων οι οποίοι καθορίζουν την ενδεδειγμένη συμπεριφορά των χρηστών και χρηστών παρόχου αναφορικά με την προστασία των κωδικών ασφάλειας. Το σύνολο των εν λόγων κανόνων, οι οποίοι αποτελούν υποσύνολο της πολιτικής δημιουργίας και διαχείρισης κωδικών ασφάλειας, συνιστούν την πολιτική προστασίας των κωδικών ασφάλειας.

(στ) Περιγραφή των διαδικασιών σύμφωνα με τις οποίες διενεργείται έλεγχος για την πιστή ή μη εφαρμογή της εν λόγω πολιτικής.

3. Η πολιτική δημιουργίας και διαχείρισης κωδικών ασφάλειας θα πρέπει να βρίσκεται καταγεγραμμένη σε αντίστοιχο επίσημο έντυπο του πάροχου διαδικτύου, στο οποίο πρέπει να υπάρχει ελεγχόμενη πρόσβαση.

4. Οι χρήστες και χρήστες παρόχου, μόλις παραλαμβάνουν τους κωδικούς ασφάλειάς τους, θα πρέπει να λαμβάνουν εγγράφως γνώση των υποχρεώσεών τους που απορρέουν από τις υφιστάμενες πολιτικές για τους κωδικούς ασφάλειας.

5. Η πολιτική δημιουργίας και διαχείρισης κωδικών ασφάλειας θα πρέπει να πληροί, κατ' ελάχιστον, τα ακόλουθα χαρακτηριστικά:

(α) Ύπαρξη συμπαγών κωδικών ασφάλειας: Οι χρησιμοποιούμενοι κωδικοί ασφάλειας θα πρέπει να είναι συμπαγείς έτσι ώστε να μην μπορεί να τους «μαντέψει» όποιος επιβουλεύεται το σύστημα. Συνεπώς η πολιτική κωδικών ασφάλειας θα πρέπει να επιβάλλει τη δημιουργία κωδικών ασφάλειας με συνδυασμό γραμμάτων, αριθμών και μη αλφαριθμητικών χαρακτήρων. Επιπλέον θα πρέπει να επιβάλλεται ένα ικανό ελάχιστο μήκος.

(β) Περιορισμένη πρόσβαση στο αρχείο φύλαξης των κωδικών ασφάλειας: Η πρόσβαση στο αρχείο που φυλάσσονται οι κωδικοί πρόσβασης θα πρέπει να είναι περιορισμένη.

(γ) Περιοδική αλλαγή κωδικών ασφάλειας: Η πολιτική θα πρέπει να μην ευνοεί την συνεχή χρήση του ιδίου κωδικού ασφάλειας. Η συχνότητα με την οποία επιβάλλεται στους χρήστες και στους χρήστες παρόχου να αλλάζουν κωδικό εξαρτάται από τους διαχειριστές του συστήματος καθώς και από τη φύση της λειτουργίας του παρόχου διαδικτύου. Πάντως σε χαρακτηριστικές περιπτώσεις όπως είναι (ενδεικτικά) η αποχώρηση κάποιου χρήστη παρόχου ή η παραβίαση κάποιου λογαριασμού τότε θα πρέπει άμεσα να λαμβάνει χώρα αλλαγή του αντίστοιχου κωδικού ασφάλειας. Επιπλέον σε περιπτώσεις ευρείας παραβίασης της ασφάλειας του συστήματος, η οποία ενδέχεται να περιλαμβάνει και παραβίαση λογαριασμών διαχειριστών του συστήματος, θα πρέπει να λαμβάνει χώρα αλλαγή όλων των κωδικών ασφάλειας.

(δ) Αδρανοποίηση κωδικού ασφάλειας: Ως επιπλέον μέτρο ασφάλειας δύναται να επιβληθεί η αδρανοποίηση του λογαριασμού του χρήστη και του χρήστη παρόχου στην περίπτωση επαναλαμβανόμενης εισαγωγής κωδικών ασφάλειας (π.χ. μετά από τρεις συνεχόμενες αποτυχημένες απόπειρες).

6. Οι υπεύθυνοι ασφάλειας του συστήματος οφείλουν να πραγματοποιούν περιοδικούς ελέγχους προκειμένου να διαπιστώσουν κατά πόσον οι κωδικοί ασφάλειας είναι συμπαγείς με βάση τους αντιστοίχους κανόνες της πολιτικής δημιουργίας και διαχείρισης κωδικών ασφάλειας. Οι έλεγχοι θα περιλαμβάνουν δοκιμές της αντοχής στις μεθόδους αποκρυπτογράφησης των υφισταμένων κωδικών με αυτοματοποιημένο τρόπο μέσω καταλλήλων εργαλείων λογισμικού.

7. Εφόσον κατά τη διάρκεια των περιοδικών ελέγχων διαπιστωθεί η ύπαρξη μη συμπαγών κωδικών ασφάλειας, οι αντίστοιχοι χρήστες θα υποχρεώνονται να προβούν άμεσα στην αντικατάστασή τους.

Άρθρο 12
Δημιουργία και Διαχείριση κωδικών ασφάλειας αναφορικά με την πρόσβαση (μέσω Διαδικτύου) από απόσταση σε εφαρμογές

1. Εφόσον ένας πάροχος διαδικτύου παρέχει στους χρήστες και χρήστες παρόχου πρόσβαση από απόσταση (μέσω Διαδικτύου) σε εφαρμογές, θα πρέπει να λαμβάνει επιπλέον μέτρα σε σχέση με τη δημιουργία και διαχείριση των κωδικών ασφάλειας.

2. Στο βαθμό που είναι τεχνικά δυνατόν θα πρέπει να υφίσταται μία κοινή αρχιτεκτονική ταυτοποίησης για όλες τις εφαρμογές στις οποίες παρέχεται πρόσβαση μέσω Διαδικτύου. Η εν λόγω αρχιτεκτονική είναι προτιμότερο να βασίζεται σε διεθνώς αποδεκτά πρότυπα (π.χ. RADIUS)

3. Οι υπεύθυνοι ασφάλειας του παρόχου διαδικτύου θα πρέπει να προβαίνουν σε αποτίμηση κινδύνου αναφορικά με το κατά πόσον μια τέτοια εφαρμογή καθίσταται ασφαλής μέσω της χρήσης ονόματος χρήστη / κωδικού ασφάλειας ή κατά πόσον θα πρέπει να χρησιμοποιούνται πρόσθετες τεχνικές ταυτοποίησης. Χαρακτηριστικό παράδειγμα αποτελούν οι εφαρμογές μέσω των οποίων λαμβάνουν χώρα οικονομικές συναλλαγές.

4. Η εν λόγω αποτίμηση θα πρέπει μεταξύ άλλων να παρέχει κατευθύνσεις αναφορικά με τα ακόλουθα:

(α) Κατά πόσον οι εν λόγω εφαρμογές είναι σχεδιασμένες με βάση την εγκεκριμένη πολιτική για τους κωδικούς ασφάλειας.

(β) Ποιες εφαρμογές θα πρέπει να υποστηρίζουν την κρυπτογράφηση του ζεύγους αναγνωριστικών όνομα χρήστη / κωδικός ασφάλειας κατά την πρόσβαση στην εφαρμογή μέσω της χρήσης καταλλήλου πρωτοκόλλου βασισμένο σε αλγόριθμο κρυπτογράφησης δημοσίου κλειδιού (π.χ. https).

(γ) Για ποιες εφαρμογές απαιτείται να παράγεται εκ νέου κωδικός ασφάλειας κάθε φορά που κάποιος χρήστης χρειάζεται να αποκτήσει πρόσβαση από απόσταση σε αυτές. Σε μια τέτοια περίπτωση θα πρέπει να προδιαγράφεται η διαδικασία δημιουργίας τέτοιων βραχύβιων κωδικών, π.χ. μέσω της χρήσης εξειδικευμένων συσκευών που διατίθενται στους χρήστες και στους χρήστες παρόχου.

5. Στις περιπτώσεις όπου υφίστανται εφαρμογές οι οποίες υποστηρίζουν αποκρυπτογράφηση δεδομένων με χρήση ιδιωτικού κλειδιού, οι πολιτικές που ισχύουν για τη διαχείριση των κωδικών ασφάλειας έχουν εφαρμογή και στη διαχείριση των ιδιωτικών κλειδιών.

Άρθρο 13
Προστασία κωδικών ασφάλειας

1. Οι υπεύθυνοι ασφάλειας του δικτύου ή του συστήματος θα πρέπει να δίνουν έμφαση στην ενημέρωση των χρηστών αναφορικά με την πολιτική προστασίας των κωδικών ασφάλειας.

2. Συνιστάται η πολιτική προστασίας των κωδικών ασφάλειας να είναι καταγεγραμμένη με τη μορφή απλών κανόνων οι οποίοι θα είναι κατανοητοί από το σύνολο των χρηστών και χρηστών παρόχου έτσι ώστε να μπορούν να τους εφαρμόζουν.

3. Η πολιτική προστασίας των κωδικών ασφάλειας θα πρέπει να περιλαμβάνει, κατ' ελάχιστον, τους ακόλουθους κανόνες:

(α) Ο χρήστης και χρήστης παρόχου δεν θα πρέπει να μοιράζεται των κωδικό ασφάλειας του με άλλους χρήστες και χρήστες παρόχου εκτός αν ο λογαριασμός στον οποίο αντιστοιχεί ο εν λόγω κωδικός προορίζεται ρητώς για πρόσβαση πολλαπλών χρηστών.

(β) Ο χρήστης και χρήστης παρόχου δεν θα πρέπει να αποκαλύπτει σε οποιονδήποτε τον κωδικό ή τους κωδικούς ασφάλειας που του έχουν δοθεί. Η απαγόρευση αυτή περιλαμβάνει και άτομα που υπό άλλες συνθήκες θεωρούνται έμπιστα όπως π.χ. προϊσταμένους, υφισταμένους, φίλους και μέλη της οικογένειας του χρήστη και χρήστη παρόχου.

(γ) Ο χρήστης και χρήστης παρόχου δεν θα πρέπει να συμπεριλαμβάνει τους κωδικούς ασφάλειάς του σε μηνύματα ηλεκτρονικού ταχυδρομείου.

(δ) Ο χρήστης και χρήστης παρόχου δεν θα πρέπει να αναφέρει τους κωδικούς ασφάλειας του κατά τη διάρκεια τηλεφωνικών συνομιλιών.

(ε) Ο χρήστης και χρήστης παρόχου δεν θα πρέπει να καταγράφει τους κωδικούς ασφάλειας του σε ερωτηματολόγια ή άλλα έγγραφα ακόμα και αν αυτά αποτελούν επίσημα έγγραφα του παρόχου διαδικτύου.

(στ) Ο χρήστης και χρήστης παρόχου δεν θα πρέπει να χρησιμοποιεί τον κωδικό ασφάλειάς του προκειμένου να παρέχει πρόσβαση στο σύστημα σε μη εξουσιοδοτημένα άτομα.

(ζ) Ο χρήστης και χρήστης παρόχου οφείλει να απομνημονεύει τον κωδικό ασφάλειας του. Ως εκ τούτου, δεν θα πρέπει να καταγράφει τον κωδικό ασφάλειας του σε χαρτί ή άλλο μέσο καταγραφής ιδιαίτερα εφόσον το μέσο καταγραφής βρίσκεται κοντά στον υπολογιστή του. Σε περίπτωση που, για οποιονδήποτε λόγο, η απομνημόνευση είναι αδύνατη τότε το μέσο καταγραφής του κωδικού ασφάλειας θα πρέπει να τοποθετείται σε κάποιον προστατευμένο χώρο (π.χ. κλειδωμένη ντουλάπα)

(η) Ο χρήστης και χρήστης παρόχου οφείλει να αναφέρει στους υπευθύνους ασφάλειας οποιοδήποτε γεγονός ή ενέργεια υποπέσει στην αντίληψη του σχετικά με την παραβίαση της ασφάλειας του λογαριασμού του.

4. Η πολιτική προστασίας κωδικών ασφάλειας θα πρέπει να αναφέρει ρητώς τις επιβαλλόμενες κυρώσεις για τις περιπτώσεις που διαπιστωθεί παράβαση της εν λόγω πολιτικής εξ' υπαιτιότητος του χρήστη και χρήστη παρόχου.

ΚΕΦΑΛΑΙΟ VI
ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΠΟΤΡΟΠΗ ΙΩΝ

Άρθρο 14
Σκοπός και Αναγκαιότητα της Πολιτικής

1. Η Πολιτική Προστασίας και Αποτροπής Ιών (Anti-virus Policy) περιγράφει τις διαδικασίες αποτροπής, ανίχνευσης και αντιμετώπισης ιών που απαιτούνται προκειμένου να εξασφαλίζεται στο μέγιστο δυνατό βαθμό η προστασία του συνόλου του δικτύου του παρόχου διαδικτύου και των χρηστών του από ιούς.

2. Σε ό,τι αφορά τη διασφάλιση απορρήτου επικοινωνιών ενός χρήστη και χρήστη παρόχου, πολλοί ιοί παραβιάζουν το σύστημα ασφάλειας του υπολογιστικού συστήματος και δημιουργούν αδυναμίες, μέσω των οποίων είναι δυνατόν να εγκατασταθούν προγράμματα πάσης φύσεως συμπεριλαμβανομένου και εφαρμογών που αποσκοπούν στην:

(α) Καταστροφή διαβαθμισμένων - απόρρητων πληροφοριών
(β) Υποκλοπή διαβαθμισμένων - απόρρητων πληροφοριών
(γ) Παρακολούθηση και καταγραφή των ενεργειών του χρήστη και χρήστη παρόχου
(δ) Υποκλοπή διαβαθμισμένων - απόρρητων επικοινωνιών
(ε) Αδυναμία πρόσβασης σε διαβαθμισμένες - απόρρητες πληροφορίες

3. Για να επιτευχθεί η προστασία από τους ιούς, ο πάροχος διαδικτύου, ο χρήστης και ο χρήστης παρόχου οφείλουν να ακολουθήσουν συγκεκριμένες διαδικασίες αποτροπής, ανίχνευσης και αντιμετώπισης των ιών, όπως περιγράφεται στις παραγράφους που ακολουθούν.

4. Ο πάροχος διαδικτύου είναι υποχρεωμένος να διαθέτει «Πολιτική Προστασίας Ιών» στην οποία οφείλει να δημοσιεύει όλες τις διαδικασίες αποτροπής, ανίχνευσης και αντιμετώπισης ιών που εφαρμόζει και είναι σύμφωνες με τις παραγράφους που ακολουθούν.

Άρθρο 15
Υποχρεώσεις του Παρόχου Διαδικτύου

1. Αποτροπή Ιών από τον πάροχο διαδικτύου: Ο πάροχος διαδικτύου οφείλει να:

(α) Διαθέτει δικτυακό εξοπλισμό ο οποίος περιορίζει την μετάδοση ιών. Για παράδειγμα, η μετάδοση ορισμένων ιών είναι δυνατόν να περιοριστεί μέσω χρήσης ειδικών φίλτρων (firewalls) στη δικτυακή υποδομή του παρόχου διαδικτύου. Η αναγκαία παραμετροποίηση των ειδικών αυτών φίλτρων πρέπει να εφαρμόζεται έγκαιρα και να διατηρείται έως ότου ο κίνδυνος από το συγκεκριμένο ιό έχει περιοριστεί. Ενδεικτικά, συνίσταται η διατήρηση των ειδικών παραμέτρων για δύο τουλάχιστον εβδομάδες.

(β) Διαθέτει το απαραίτητο λογισμικό για την προστασία από ιούς όλων των υπηρεσιών και εφαρμογών που προσφέρει στους χρήστες. Για παράδειγμα, υπηρεσίες όπως το ηλεκτρονικό ταχυδρομείο (e-mail) πρέπει να προστατεύονται από εξειδικευμένο λογισμικό (e-mail scanners).

(γ) Εγκαθιστά μονίμως στη μνήμη (memory resident) των υπολογιστικών συστημάτων λογισμικό προστασίας από ιούς, το οποίο να εξετάζει αυτομάτως όλα τα εισερχόμενα δεδομένα.

(δ) Εκπαιδεύει και ελέγχει τους χρήστες παρόχου σε τακτά χρονικά διαστήματα, ώστε να ακολουθούνται πάντα οι παραπάνω πολιτικές αποτροπής ιών.

(ε) Διατηρεί μια ομάδα ειδικών για την προστασία από ιούς, η οποία θα φροντίζει να ενημερώνεται σχετικά με την πιθανότητα επίθεσης από νέους ιούς (με σκοπό την έγκαιρη εγκατάσταση ή/και παραμετροποίηση των απαραίτητων μέσων προστασίας) και θα επανεξετάζει περιοδικά (τουλάχιστον 2 φορές το χρόνο) την πολιτική προστασίας ιών.

(στ) Ενημερώνει κι εκπαιδεύει τους χρήστες και χρήστες παρόχου σχετικά με το πώς μπορούν να προστατευθούν από τους ιούς.

2. Ανίχνευση Ιών από τον πάροχο διαδικτύου: Ο πάροχος διαδικτύου οφείλει να:

(α) Ανανεώνει τα συστήματα προστασίας από ιούς (ειδικό λογισμικό και ειδικός δικτυακός εξοπλισμός) ανά τακτά χρονικά διαστήματα ώστε να μπορούν να αποτρέψουν τη μετάδοση νέων ιών. Συνίσταται η αυτόματη ενημέρωση των συστημάτων του παρόχου διαδικτύου ανά δώδεκα (12) ώρες.

(β) Εξασφαλίζει ότι όλα τα αρχεία που είναι αποθηκευμένα στα συστήματα του παρόχου διαδικτύου και τα οποία είναι πιθανόν να περιλαμβάνουν ιούς εξετάζονται καθημερινά από προγράμματα ανίχνευσης ιών.

(γ) Ενημερώνει τους χρήστες και χρήστες παρόχου το δυνατόν συντομότερο σε περιπτώσεις όπου υπάρχει έξαρση μετάδοσης κάποιου επικίνδυνου ιού. Η ενημέρωση αυτή είναι δυνατόν να γίνεται με διάφορους τρόπους. Συνίσταται η ενημέρωση να γίνεται μέσω ηλεκτρονικού ταχυδρομείου, με ταυτόχρονη παρουσίαση του προβλήματος στην κεντρική σελίδα του δικτυακού του τόπου. Ο πάροχος διαδικτύου πρέπει να δίνει πληροφορίες για την αντιμετώπιση του ιού παρέχοντας links σε δικτυακούς τόπους μέσω των οποίων ο χρήστης και ο χρήστης παρόχου μπορεί να βρει το απαραίτητο λογισμικό για την αντιμετώπιση του ιού.

(δ) Ενημερώνει τους χρήστες και χρήστες παρόχου σχετικά με περιπτώσεις φάρσας, όπου ο χρήστης γίνεται συνήθως αποδέκτης ενός email που τον προειδοποιεί για την ύπαρξη κάποιου υποτιθέμενου ιού στο υπολογιστικό του σύστημα και τον παροτρύνει να προβεί σε ενέργειες, οι οποίες τελικά προκαλούν βλάβη στην σωστή λειτουργία του λειτουργικού συστήματος.

3. Αντιμετώπιση Ιών από τον πάροχο διαδικτύου: Ο πάροχος διαδικτύου οφείλει να:

(α) Ορίσει ομάδα αντιμετώπισης ιών, η οποία θα αναλαμβάνει την ανίχνευση και αφαίρεση όλων των ιών από τα υπολογιστικά συστήματα του παρόχου διαδικτύου.

(β) Απομονώνει εκτός δικτύου υπολογιστικά συστήματα στα οποία ανιχνεύθηκε κάποιος ιός. Το σύστημα είναι απαραίτητο να παραμείνει εκτός δικτύου ωσότου ο ιός αφαιρεθεί ολοκληρωτικά.

(γ) Στην περίπτωση που κάποιος χρήστης ζητήσει βοήθεια (είτε τηλεφωνικά είτε μέσω άλλου τρόπου επικοινωνίας) από τον πάροχο διαδικτύου για την αντιμετώπιση ιών, ο πάροχος διαδικτύου πρέπει να είναι προετοιμασμένος να παραπέμψει τον χρήστη σε πληροφοριακές ιστοσελίδες και σε εταιρείες που προσφέρουν αντίστοιχες υπηρεσίες.

Άρθρο 16
Συστάσεις προς τον Χρήστη και Χρήστη Παρόχου

1. Αποτροπή Ιών: Ο χρήστης και ο χρήστης παρόχου συνίσταται να:

(α) Αναζητά βοήθεια από τον πάροχο διαδικτύου ή οποιονδήποτε άλλο οργανισμό μπορεί να βοηθήσει σχετικά με οποιαδήποτε μη φυσιολογική συμπεριφορά του λειτουργικού του συστήματος ή εφαρμογής.

(β) Έχει εγκατεστημένο μονίμως στην μνήμη (memory resident) ειδικό λογισμικό προστασίας από ιούς.

2. Ανίχνευση Ιών: Ο χρήστης και ο χρήστης παρόχου συνίσταται να:

(α) Χρησιμοποιεί την υπηρεσία αυτόματης ενημέρωσης του λογισμικού για νέους ιούς τουλάχιστον μια φορά το μήνα.

(β) Εξετάζει όλα τα αρχεία του προσωπικού υπολογιστή τουλάχιστον 2 φορές τον μήνα.

3. Αντιμετώπιση Ιών: Ο χρήστης και ο χρήστης παρόχου συνίσταται να:

(α) Αποσυνδέει το υπολογιστικό του σύστημα από το δίκτυο μέχρις ότου ο ιός αφαιρεθεί ολοκληρωτικά.

(β) Σε κάθε περίπτωση ο χρήστης και ο χρήστης παρόχου έχει το δικαίωμα να επικοινωνήσει με τον πάροχο διαδικτύου του και να ζητήσει πληροφορίες για την αντιμετώπιση των ιών. Ο πάροχος διαδικτύου σε αυτή την περίπτωση είναι υποχρεωμένος να παρέχει βοήθεια στο χρήστη και στο χρήστη παρόχου παραπέμποντας τον σε αντίστοιχες ιστοσελίδες ή και σε εταιρείες που προσφέρουν αντίστοιχες υπηρεσίες.

4. Υπενθυμίζεται ότι η σκόπιμη παραγωγή και μετάδοση ιών από συγκεκριμένο άτομο φέρει βαριές κυρώσεις μέσω της είδη υπάρχουσας νομοθεσίας.

ΚΕΦΑΛΑΙΟ VII
ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΑΡΟΧΟΥ ΥΠΗΡΕΣΙΑΣ ΕΦΑΡΜΟΓΗΣ (APPLICATION SERVICE PROVIDER)

Άρθρο 17
Σκοπός και Εφαρμογή της Πολιτικής

1. Η πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής ορίζει το σύνολο των εγγυήσεων που οφείλει να λαμβάνει ο πάροχος διαδικτύου από τον πάροχο υπηρεσίας εφαρμογής, προκειμένου να εξασφαλιστεί το απόρρητο των επικοινωνιών των χρηστών. Η πολιτική αυτή ισχύει σε περίπτωση που ο πάροχος διαδικτύου και ο πάροχος υπηρεσίας εφαρμογής έχουν συμβατική σχέση, ανεξαρτήτως της τοποθεσίας όπου φιλοξενείται η υποδομή που υποστηρίζει τις εν λόγω υπηρεσίες και εφαρμογές.

2. Ο πάροχος διαδικτύου είναι υποχρεωμένος να διαθέτει και να εφαρμόζει πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής, η οποία να διασφαλίζει το απόρρητο των επικοινωνιών των χρηστών και να είναι σύμφωνη με τις παραγράφους που ακολουθούν.

3. Η ανάθεση μιας υπηρεσίας σε κάποιον πάροχο υπηρεσίας εφαρμογής πρέπει να γίνεται ύστερα από γραπτή έγκριση του Νομικού Εκπροσώπου του παρόχου διαδικτύου.

4. Ο πάροχος διαδικτύου οφείλει να ελέγχει διεξοδικά κατά πόσο ο πάροχος υπηρεσίας εφαρμογής δύναται να εφαρμόσει την πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής πριν την ανάθεση της υπηρεσίας και κατά τη διάρκεια λειτουργίας της υπηρεσίας. Ο πάροχος διαδικτύου είναι ο τελικός υπεύθυνος για την εφαρμογή της πολιτικής αυτής από τον πάροχο υπηρεσίας εφαρμογής.

5. Υπεύθυνος για τον ορισμό, έλεγχο εφαρμογής και οποιαδήποτε αλλαγή της πολιτικής ασφάλειας παρόχου υπηρεσίας εφαρμογής ορίζεται ο Υπεύθυνος Ασφάλειας του παρόχου διαδικτύου.

6. Ο πάροχος διαδικτύου επιτρέπεται να παραδίδει απόρρητα δεδομένα χρήστη στον πάροχο υπηρεσίας εφαρμογής μόνο εφόσον ο χρήστης έχει λάβει σαφείς πληροφορίες για τον σκοπό της επεξεργασίας, και πάντα με τη συγκατάθεση αυτού. Αυτό βέβαια δεν ισχύει στην περίπτωση που οι ενέργειες αυτές γίνονται για την εξυπηρέτηση της υπηρεσίας που έχει ρητά ζητήσει ο χρήστης.

7. Ο πάροχος διαδικτύου έχει το δικαίωμα να εξετάζει ανά τακτά χρονικά διαστήματα το κατά πόσο ο πάροχος υπηρεσίας εφαρμογής εφαρμόζει την πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής. Αν ο έλεγχος απαιτεί φυσική παρουσία στις εγκαταστάσεις του παρόχου υπηρεσίας εφαρμογής, ο πάροχος διαδικτύου οφείλει να ενημερώσει τον πάροχο υπηρεσίας εφαρμογής τουλάχιστον 24 ώρες πριν, ειδάλλως δεν απαιτείται καμία προειδοποίηση.

8. Ο πάροχος υπηρεσίας εφαρμογής οφείλει να καταθέσει στον πάροχο διαδικτύου το πλήρες διάγραμμα δικτύου που χρησιμοποιεί για την υποστήριξη της εν λόγω υπηρεσίας, καθώς και τις τυχόν διασυνδέσεις του δικτύου αυτού με άλλα δίκτυα του παρόχου υπηρεσίας εφαρμογής και του παρόχου διαδικτύου. Θα πρέπει επίσης να κατατίθεται το πλήρες διάγραμμα ροής που αφορά στα απόρρητα δεδομένα επικοινωνιών, συμπεριλαμβανομένου των μέσων αποθήκευσης, εφαρμογών επεξεργασίας και μέτρων ασφάλειας των δεδομένων αυτών.

9. Ο πάροχος υπηρεσίας εφαρμογής οφείλει να διακόπτει άμεσα τη λειτουργία της υπηρεσίας σε περίπτωση που εντοπιστεί οποιοδήποτε θέμα ασφάλειας των απόρρητων δεδομένων επικοινωνίας.

10. Ο πάροχος υπηρεσίας εφαρμογής οφείλει να ενημερώνει τον Υπεύθυνο Ασφάλειας του παρόχου διαδικτύου σχετικά με όλα τα συμβάντα ασφάλειας που αφορούν στα απόρρητα δεδομένα επικοινωνιών.

11. Σε ό,τι αφορά θέματα πρόσβασης στις εφαρμογές λογισμικού, την υλική υποδομή και το δίκτυο του παρόχου υπηρεσίας εφαρμογής, η πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής πρέπει να περιλαμβάνει τουλάχιστον τα παρακάτω:

(α) Ο πάροχος υπηρεσίας εφαρμογής οφείλει να εφαρμόζει την Πολιτική Πρόσβασης του παρόχου διαδικτύου ως προς τα συστήματα αποθήκευσης, επεξεργασίας και μεταφοράς των απόρρητων δεδομένων επικοινωνιών.

(β) Ο πάροχος διαδικτύου έχει τον τελικό λόγο σε θέματα πρόσβασης (φυσικής και μη) στα συστήματα αποθήκευσης, επεξεργασίας και μεταφοράς των απόρρητων δεδομένων επικοινωνιών.

(γ) Ο πάροχος υπηρεσίας εφαρμογής οφείλει να γνωστοποιεί στον πάροχο διαδικτύου το προσωπικό το οποίο θα έχει φυσική και μη πρόσβαση στα συστήματα αποθήκευσης, επεξεργασίας και μεταφοράς των απόρρητων δεδομένων επικοινωνιών.

12. Ο πάροχος υπηρεσίας εφαρμογής υποχρεούται να χρησιμοποιεί διαδικασίες και μεθόδους κρυπτογράφησης των απόρρητων δεδομένων επικοινωνίας, όπως αυτές ορίζονται στην Πολιτική Χρήσης Κρυπτογραφικών Αλγορίθμων του παρόχου διαδικτύου.

13. Ο πάροχος υπηρεσίας εφαρμογής οφείλει να εφαρμόζει την Πολιτική Κωδικών (Password Policy) του παρόχου διαδικτύου ως προς τα συστήματα αποθήκευσης, επεξεργασίας και μεταφοράς των απόρρητων δεδομένων επικοινωνιών.

14. Ο πάροχος υπηρεσίας εφαρμογής οφείλει να ενημερώνει εγγράφως τον πάροχο διαδικτύου ως προς τις διαδικασίες ελέγχου ασφάλειας που ακολουθεί σχετικά με την επαλήθευση ταυτότητας (authentication), εξουσιοδότηση (authorization) και αποκάλυψη κενών ασφάλειας των εφαρμογών παγκόσμιου ιστού (WWW).

15. Ο πάροχος διαδικτύου οφείλει να έχει την έγγραφη διαβεβαίωση του παρόχου υπηρεσίας εφαρμογής σχετικά με την αποδοχή και πλήρη εφαρμογή των μέτρων διασφάλισης του απορρήτου των επικοινωνιών που περιγράφονται στις προηγούμενες παραγράφους.

16. Η πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής συνίσταται να ορίζει χρηματικές ποινές, ακόμα και την κατάργηση του συμβολαίου, για την περίπτωση κατά την οποία ο πάροχος υπηρεσίας εφαρμογής παραβεί τα μέτρα διασφάλισης του απορρήτου των επικοινωνιών.

ΚΕΦΑΛΑΙΟ VIII
ΔΙΑΔΙΚΑΣΙΑ ΣΥΜΒΑΣΗΣ ΥΠΕΡΓΟΛΑΒΙΑΣ

Άρθρο 18
Σύμβαση υπεργολαβίας με σκοπό την διασφάλιση απορρήτου

1. Σε κάθε περίπτωση όπου ο πάροχος διαδικτύου προβαίνει σε συμφωνία με τον εκάστοτε υπεργολάβο για την ανάληψη έργου το οποίο απαιτεί πρόσβαση σε εξοπλισμό ή λογισμικό το οποίο περιέχει ή παρέχει πρόσβαση σε διαβαθμισμένα, ευαίσθητα ή απόρρητα δεδομένα, ο πάροχος διαδικτύου είναι υποχρεωμένος να διαφυλάσσει το απόρρητο των πληροφοριών.

2. Για την διασφάλιση του απορρήτου υπό συνθήκες υπεργολαβίας απαιτείται η υπογραφή συμβάσεως προστασίας του απορρήτου των πληροφοριών. Ιδιαίτερη προσοχή πρέπει να δίνεται στη διασφάλιση του απορρήτου των επικοινωνιών, σε περιπτώσεις που απαιτείται πρόσβαση από τον υπεργολάβο σε εξοπλισμό ή λογισμικό το οποίο χρησιμοποιείται στις επικοινωνίες ή αποθηκεύει πληροφορίες επικοινωνιών.

3. Η σύμβαση μεταξύ παρόχου διαδικτύου και υπεργολάβου πρέπει να περιέχει τουλάχιστον τις παρακάτω παραγράφους.

4. Ο υπεργολάβος σε καμία περίπτωση δεν έχει το δικαίωμα να προβεί στην καταπάτηση του απορρήτου όπως αυτό περιγράφεται και διαφυλάσσεται από την είδη υπάρχουσα πολιτική ασφάλειας του παρόχου διαδικτύου.

5. Ο υπεργολάβος έχει λάβει γνώση της υπάρχουσας πολιτικής προστασίας του απορρήτου των τηλεπικοινωνιών του παρόχου διαδικτύου, και ενυπόγραφα συμφωνεί με τους όρους, προϋποθέσεις και περιορισμούς που επιβάλλονται από την πολιτική αυτή.

6. Το εκάστοτε πρόσωπο το οποίο εν τέλει θα έχει πρόσβαση στον ευαίσθητο εξοπλισμό / λογισμικό έχει λάβει ειδική άδεια από τον πάροχο διαδικτύου (και όχι τον υπεργολάβο) αφού πρώτα έχει ενημερωθεί, συμφωνήσει και συνυπογράψει την σύμβαση διασφάλισης απορρήτου.

7. Ο υπεργολάβος πρέπει να έχει την άδεια του παρόχου διαδικτύου για να εκχωρήσει δικαιώματα χρήσης του ευαίσθητου εξοπλισμού σε τρίτους (εργολάβους). Κατά την εκάστοτε εκχώρηση δικαιωμάτων σε τρίτους επιβάλλεται να διατηρείται το ίδιο επίπεδο διασφάλισης του απορρήτου και να υπογράφονται αντίστοιχα συμφωνητικά μεταξύ των τρίτων και του παρόχου διαδικτύου. Ο υπεργολάβος σε καμιά περίπτωση δεν είναι εξουσιοδοτημένος να παραχωρήσει αυτός δικαιώματα χρήσης. Πάντοτε η εκχώρηση δικαιωμάτων γίνεται από τον κύριο του έργου, δηλαδή τον πάροχο διαδικτύου και μόνο.

8. Ο πάροχος διαδικτύου ορίζει συγκεκριμένο φυσικό πρόσωπο που είναι υπεύθυνο για την εποπτεία του υπεργολάβου καθώς και των τυχόν εργολάβων σε ζητήματα διασφάλισης απορρήτου, ο οποίος ονομάζεται Επόπτης Ασφάλειας.

9. Τυχόν παραβίαση των κανόνων από τον υπεργολάβο χρίζει άμεσης καταγγελίας στην ΑΔΑΕ από τον καθορισμένο Επόπτη Ασφάλειας.

ΚΕΦΑΛΑΙΟ IX
ΕΛΕΓΧΟΣ ΚΑΙ ΕΠΟΠΤΕΙΑ

Άρθρο 19
Γενικά

1. Οι πολιτικές που ορίστηκαν στον κανονισμό αυτό αποτελούν μέρος της γενικότερης Πολιτικής Ασφάλειας του παρόχου διαδικτύου, όπως αυτή ορίστηκε στον «Κανονισμό για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές».

2. Κατά συνέπεια, η ΑΔΑΕ στα πλαίσια ελέγχου και εποπτείας που καθορίστηκαν στον «Κανονισμό για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές», μπορεί ανά πάσα στιγμή να προβεί σε έλεγχο του καθορισμού, επιβολής και σωστής λειτουργίας των πολιτικών που ορίστηκαν στον κανονισμό αυτό.

3. Σχετικά με τις λεπτομερείς διαδικασίες διενέργειας του ελέγχου καθώς και τις προβλεπόμενες διοικητικές κυρώσεις ισχύουν, κατ' αναλογία, τα αναγραφόμενα στον «Κανονισμό για την Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές».

Άρθρο 20
Πολιτική Χρήσης Κρυπτογραφικών Αλγορίθμων

1. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να ζητήσει πλήρη ενημέρωση από τους παρόχους διαδικτύου και από τους παρόχους υπηρεσίας εφαρμογής σχετικά με την τεχνική ή αλγόριθμο κρυπτογράφησης που χρησιμοποιεί στα συστήματα μετάδοσης ή ανά πεδίο εφαρμογής καθώς και το μήκος του κλειδιού.

2. Η ΑΔΑΕ μπορεί να κάνει αυτοψία για να διαπιστώσει αν όντως εφαρμόζονται οι τεχνικές κρυπτογράφησης όπως δηλώνονται από τους πάροχους διαδικτύου και τους πάροχους υπηρεσίας εφαρμογής.

Άρθρο 21
Πολιτική Προστασίας Κωδικών Ασφάλειας

1. Η ΑΔΑΕ δύναται ανά πάσα στιγμή να διενεργήσει έλεγχο σε οποιονδήποτε φορέα εμπίπτει στη δικαιοδοσία της αναφορικά με την πολιτική κωδικών ασφάλειας.

2. Ο υπό έλεγχο φορέας οφείλει να παραδώσει στα στελέχη της ΑΔΑΕ όλα τα έντυπα στα οποία έχουν καταγραφεί οι πολιτικές κωδικών ασφάλειας καθώς και τυχόν σχετικό συνοδευτικό υλικό, π.χ. έγγραφα με οδηγίες και φόρμες που δίδονται στους χρήστες.

Άρθρο 22
Πολιτική Προστασίας από Ιούς

1. Η ΑΔΑΕ μπορεί να κάνει αυτοψία για να διαπιστώσει αν όντως ο πάροχος εφαρμόζει Πολιτική Προστασίας από Ιούς, διαθέτει απαραίτητα συστήματα προστασίας από ιούς (ειδικό λογισμικό και ειδικός δικτυακός εξοπλισμός) και ακολουθεί τις διαδικασίες που περιγράφονται στις αντίστοιχες διατάξεις του παρόντος.

2. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην Πολιτική Προστασίας από Ιούς, έτσι ώστε να είναι σε πλήρη αντιστοιχία με τις εκάστοτε νέες τεχνολογίες προσβολής και προστασίας των υπολογιστικών συστημάτων από ιούς. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος οφείλει να προσαρμόζει την Πολιτική Προστασίας από Ιούς αναλόγως, εντός της προθεσμίας που θα ορίζεται από το κείμενο τροποποίησης.

Άρθρο 23
Πολιτική Ασφάλειας Παρόχου Υπηρεσίας Εφαρμογής

1. Η ΑΔΑΕ μπορεί να κάνει αυτοψία για να διαπιστώσει αν όντως ο πάροχος διαδικτύου διαθέτει και εφαρμόζει

πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής σύμφωνα με τις αντίστοιχες διατάξεις του παρόντος.

2. Η ΑΔΑΕ μπορεί να κάνει αυτοψία για να διαπιστώσει αν ο πάροχος υπηρεσίας εφαρμογής εφαρμόζει την πολιτική ασφαλείας παρόχου υπηρεσίας εφαρμογής σύμφωνα με τις αντίστοιχες διατάξεις του παρόντος. Υπενθυμίζεται ότι ο πάροχος διαδικτύου είναι ο τελικός υπεύθυνος για την εφαρμογή και εποπτεία της πολιτικής αυτής από τον πάροχο υπηρεσίας εφαρμογής.

3. Η ΑΔΑΕ μπορεί ανά πάσα στιγμή να τροποποιήσει τις διατάξεις που αφορούν στην πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής. Μετά από κάθε τέτοιου είδους τροποποίηση, ο πάροχος διαδικτύου οφείλει να προσαρμόζει την πολιτική ασφάλειας παρόχου υπηρεσίας εφαρμογής και να ενημερώνει τον πάροχο υπηρεσίας εφαρμογής αναλόγως. Τόσο ο πάροχος διαδικτύου, όσο και ο πάροχος υπηρεσίας εφαρμογής οφείλουν να ολοκληρώνουν τις αλλαγές που απαιτούνται εντός της προθεσμίας που θα ορίζεται από το κείμενο τροποποίησης.

Άρθρο 24
Αρχές Πιστοποίησης

1. Σκοπός των αρχών πιστοποίησης είναι να επαληθεύουν την αντιστοιχία μιας οντότητας (π.χ. ενός φυσικού προσώπου) με το δημόσιο κλειδί της. Η επαλήθευση γίνεται με την έκδοση των λεγόμενων ψηφιακών πιστοποιητικών.

2. Οι οργανισμοί που μπορούν να δραστηριοποιηθούν στην Ελλάδα ως Αρχές Πιστοποίησης είναι υπό τον έλεγχο της ΑΔΑΕ. Η ΑΔΑΕ θα επιβλέψει ότι η αρχή πιστοποίησης είναι σύμφωνη με την υπάρχουσα νομοθεσία.

3. Η ΑΔΑΕ όποτε κρίνει απαραίτητο θα εκδίδει τεχνικούς ή μη κανονισμούς και συστάσεις που αφορούν τη λειτουργία των αρχών πιστοποίησης με κριτήριο την αξιοπιστία και την ασφαλή λειτουργία αυτών.

ΚΕΦΑΛΑΙΟ Χ
ΜΕΤΑΒΑΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 25
Μεταβατικές Διατάξεις

1. Όλοι οι πάροχοι διαδικτύου υποχρεούνται:

(α) Να ενημερώσουν ως προς την εφαρμοζόμενη πολιτική ασφάλειας την ΑΔΑΕ εντός έξι (6) μηνών από τη δημοσίευση του παρόντος.

(β) Να εφαρμόζουν την εγκριθείσα από την ΑΔΑΕ πολιτική ασφάλειας εντός ενός (1) έτους από την έγκρισή της.

ΚΕΦΑΛΑΙΟ XI
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 26
Έναρξη Ισχύος

Ο παρών Κανονισμός τίθεται σε ισχύ από την ημερομηνία δημοσίευσής του στην Εφημερίδα της Κυβερνήσεως.

Ο παρών Κανονισμός να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Αθήνα, 14 Ιανουαρίου 2005

Ο Πρόεδρος
ΑΝΔΡΕΑΣ ΛΑΜΠΡΙΝΟΠΟΥΛΟΣ